Document Number 102-95-013U

NetWare 4 Administrator's Security Guidance Handbook

Task 5
Contract No. N00039-93-C-0099
CDRL No. A003

September 5, 1995

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 71)
Arlington, VA 22245-5200

Prepared by:

Secure Solutions, Inc.

9404 Genesee Avenue, Suite 237
La Jolla, CA 92037

TEL: (619) 546-8616
FAX: (619) 546-0814

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 5, 1995	Final

4. TITLE AND SUBTITLE
Technical Report
NetWare 4 Administrator's Security Guidance Handbook

5. FUNDING NUMBERS
Contract No:
N00039-93-C-0099

6. AUTHOR(S)
Kym Blair

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Secure Solutions, Inc.
9404 Genesee Avenue, Suite 237
La Jolla, CA 92037

8. PERFORMING ORGANIZATION REPORT NUMBER
102-95-013U

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 71CE)
Arlington, VA 22245-5200

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement: Approved for Public Release; Distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Secure Solutions, Inc. was tasked by the Space and Naval Warfare Systems Command (SPAWAR) to perform a Small Business Innovation Research (SBIR) Phase II network security effort to develop NetWare 4 security guidance for environments where Sensitive Unclassified information is processed.

Approximately 60 percent of the network operating systems in operation today are Novell NetWare. Version 3, the most widely installed version, is server-centric, each server needing individual management. With NetWare 4, the most current version, administrators view the network as a single entity – *an Enterprise Network.* Government and commercial organizations face a common problem of having trained personnel rotate on to new assignments, leaving inadequately trained replacements to administer the networks. In addition, many organizations that have NetWare 3 installed are in the process of, or are contemplating, migration to NetWare 4, but their administrators have not been trained in that architecture.

This handbook provides security guidance on the implementation of NetWare 4 security features and additional third-party security products. The handbook describes basic firewall architectures and discusses issues concerning external interfaces. It also surfaces security concerns that remain in spite of the installation of NetWare features and third-party products so that the security administrator is aware of the concerns.

14. SUBJECT TERMS	15. NUMBER OF PAGES
	128
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	

Document Number 102-95-013U

NetWare 4 Administrator's Security Guidance Handbook

Task 5
Contract No. N00039-93-C-0099
CDRL No. A003

September 5, 1995

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 71)
Arlington, VA 22245-5200

Prepared by:

Secure Solutions, Inc.

9404 Genesee Avenue, Suite 237
La Jolla, CA 92037

TEL: (619) 546-8616
FAX: (619) 546-0814

Approved for public release; distribution is unlimited.

This Page Intentionally Left Blank

Table of Contents

Appendices

Appendix **Page**

Index of Figures

Figure **Page**

Index of Tables

This Page Intentionally Left Blank

Executive Summary

Secure Solutions, Inc. was tasked by the Space and Naval Warfare Systems Command (SPAWAR) to perform a Small Business Innovation Research (SBIR) Phase II research effort to develop NetWare 4 security guidance for environments where Sensitive Unclassified information is processed.

Approximately 60 percent of the network operating systems (NOSs) in operation today are Novell NetWare. NetWare 3 is currently the most widely installed version of NetWare. Version 3 is server-centric, each server needing individual management and control. NetWare 4 is Novell's most current version. With version 4, administrators view the network as a single entity – *an Enterprise Network.* User accounts are set up once and are given access rights to any servers on the network for which they are authorized. The NetWare 4 Administrator establishes access rules with one database for the entire network. This database is called *NetWare Directory Services (NDS).*

Government and commercial organizations face a common problem of having trained personnel rotate on to new assignments, leaving inadequately trained replacements to administer the networks. In addition, many organizations that have NetWare 3 installed are in the process of, or are contemplating, migration to NetWare 4, but their administrators have not been trained to manage NetWare 4.X networks.

Because NDS is complex, the administrator must take certain precautions in order to avoid unknowingly creating vulnerabilities in the security structure. In addition, there are many third-party products that can be installed to further enhance security in sensitive environments. Security issues concerning sensitive environments, NetWare 4 features, and supporting third-party products must be understood by first-time administrators as well as trained NetWare 3 administrators in order to make intelligent decisions.

This handbook is intended for the inexperienced administrator who may not have a technical background with NetWare. The objective of the handbook is to provide consolidated, concise, and easy to read security guidance on Novell NetWare 4 so that the administrator will be able to take the correct steps to counter any threats that may arise. All major security issues and topics are raised at a very high level to acquaint the new administrator with the issues. Pointers to detailed references are included for the reader who wishes to investigate specialized topics of interest to a deeper level.

The handbook goes on to discuss additional security issues that are not solved by the implementation of NetWare 4 security features, and suggests third-party products that are available to help resolve some of those problems. It also describes basic firewall architectures and discusses issues concerning external interfaces since many organizations are faced with the decision of whether to connect to external networks or remain isolated in the interest of better security. Finally, this handbook attempts to surface security concerns that remain in spite of the installation of NetWare features and third-party products so that the security administrator can at least be aware of the concerns and be alert to changes that may elevate the importance of these issues.

This Page Intentionally Left Blank

Section 1

Introduction

This Page Intentionally Left Blank

1.0 Introduction

The U.S. Navy's Space and Naval Warfare Systems Command (SPAWAR) and other commercial and Government organizations face a common problem of having personnel who are adequately trained in the administration of their organization's networks rotate on to new assignments, leaving inadequately trained replacements to administer the networks. In addition, many administrators who have been trained to manage Novell NetWare 3.X networks are being directed to upgrade their networks to NetWare 4 without obtaining further training. These trends increase the threat to data confidentiality, integrity, authenticity, and availability. This report documents the results of a study to identify and discuss the many facets of Novell NetWare security in a manner that simplifies what can be overwhelming to the first-time network administrator.

The study was performed by Secure Solutions, Inc. for SPAWAR under the Small Business Innovation Research (SBIR) Program under Contract Number N00039-93-C-0099. This introduction provides background information on why this research effort was initiated, the scope and objectives of the study, and the organization of the report.

1.1 Background

Threats are conditions which may be brought to bear against an organization's sensitive information and critical system assets to cause harm. In other words, a threat is the potential for harm. Possible harms are compromise of sensitive information, loss of data integrity, acceptance of information from a false source, and loss of resource availability. Threats are classified into two categories – natural events and human.

Nature manifests itself in the form of natural events, such as earthquake, fire, flood, or power instability. Harm is evident in the form of machine failure, such as the failure of an integrated circuit or power supply, or a failure having more subtle results. As random as nature may appear, it is statistically predictable. Natural threats are generally countered through redundancy, backup and recovery procedures, and emergency and disaster planning. Normally, threats due to nature cannot be eliminated, but safeguards and other measures to manage the natural event can be taken to prevent the (full) realization of harm. For instance, rain cannot be prevented, but computers and communications equipment can be reasonably protected from its effects.

The human threat may be malicious or inadvertent, and is further distinguished by the involvement of insiders or outsiders. As opposed to nature, the human threat can be more cunning, complex, and unpredictable. What the human threat agent lacks in sheer brute force, it more than makes up for in intelligence, technology, and motivation.

Unauthorized insider actions may be intentionally malicious, may be well intended but improper, or may be accidental. Examples include: failure to lock secure areas, sabotage of disk drives, uncoordinated or haphazard cable installation, masquerading, spoofing, network replay, and authentication violations. Spoofing (i.e., pretending to be a server or peer) requires detailed knowledge of the system and may be part of an

insider attack. It may occur in the form of a program that replaces the login program to gather usernames and passwords, a program that masquerades as a server to intercept traffic routed through it, or other program that gathers information without being detected. Insiders may also install NetWare Loadable Modules (NLMs) that call the SetBinderyObjectPassword function to change the Administrator's password without knowing the old password, or perform other covert action. NLMs are extensions of the operating system and are allowed to make system calls. Insiders may also be able to attach network analyzers (described in **Section 3.4** as an administrator's tool) to the network to passively capture clear-text passwords and data packets.

Information systems are subject to harm from insiders who are not trustworthy or adequately trained. Without the necessary levels of trust and security awareness training, personnel pose a greater risk of performing procedural errors and failing to report possible security incidents. Programmers or administrators who maintain the systems may place "Trojan Horses" or "Trap Doors" in the system. Possible motivations may be revenge (e.g., disgruntled employee), the perception of an opportunity for future gain, or an attempt to provide a safety net for recovery of the system if abnormal conditions arise. Once in place, these are very often difficult to detect and remove.

Outsiders are people who are not employees of the organization, nor maintenance or contract personnel employed by the organization. Unauthorized access or activity includes hacking through external networks or dial-in ports, theft or sabotage of tangible assets or data, and unintentional acts such as losing control of a car which results in harm to the power generation facilities through fire or explosions. Wiretapping an open telephone line can be done externally and requires no knowledge of the computer system being monitored. Unauthorized persons who pose a threat to the system include terminated employees or consultants, visitors, irate patients, vandals, computer hackers, terrorists, and social activists. In addition, outsiders may attempt to subvert insiders through "social engineering" ploys to compromise, corrupt, or delay data.

Vulnerabilities are weaknesses that threats can exploit. If there are no vulnerabilities, the threat cannot be realized and harm to the system cannot occur. The existence of a threat does not in itself imply that the system is at risk. The existence of a vulnerability does not necessarily imply that harm will occur. Threats that are capable of exploiting existing vulnerabilities must have the motivation (in the case of human threats) and the opportunity to do so before the threat can be realized. NetWare administrators must consider the threats that may exist for their organization and the vulnerabilities that may be exploited to allow those threats to be realized, and they must install the appropriate countermeasures to limit the risk.

A decade ago, centralized multi-user mainframe computers were the standard architecture for allowing users to share software applications, files, printers, and other resources. The advantages of the centralized architecture were that it allowed the sharing of data and expensive resources and provided for central control and management of the data. The disadvantages were that it was not flexible in meeting user needs and did not encourage creativity in the use of data. In addition, it was a single point of failure.

The introduction of PCs brought flexibility in the way users could manipulate their data, and also encouraged the proliferation of distributed sources of data. This often meant no central control of the information and, furthermore, it meant conflicting sources of information. In addition, it meant higher equipment costs because each user wanted a printer attached to their PC so they would not have to carry a diskette to another PC in order to print a file. Very quickly, the local area network (LAN) became popular as a tool to enable information, software, and printer sharing similar to what users experienced with the centralized architecture. The LAN combined the flexibility of desktop PCs with the sharing capabilities of the centralized processor.

Dedicated servers soon emerged because some server functions, such as database management, required more power than a non-dedicated PC could provide. As depicted in **Figure 1-1**, many functions have been migrated to dedicated servers. For example, dedicated servers are used to support not only application files, databases, and print spooling, but also central LAN management and security, fax machines, graphic scanning, mailboxes, dial-up modems, and directory services. Even dumb terminals can still access a centralized host connected to the LAN through the use of terminal servers. Client-server strategies create relatively inexpensive computing

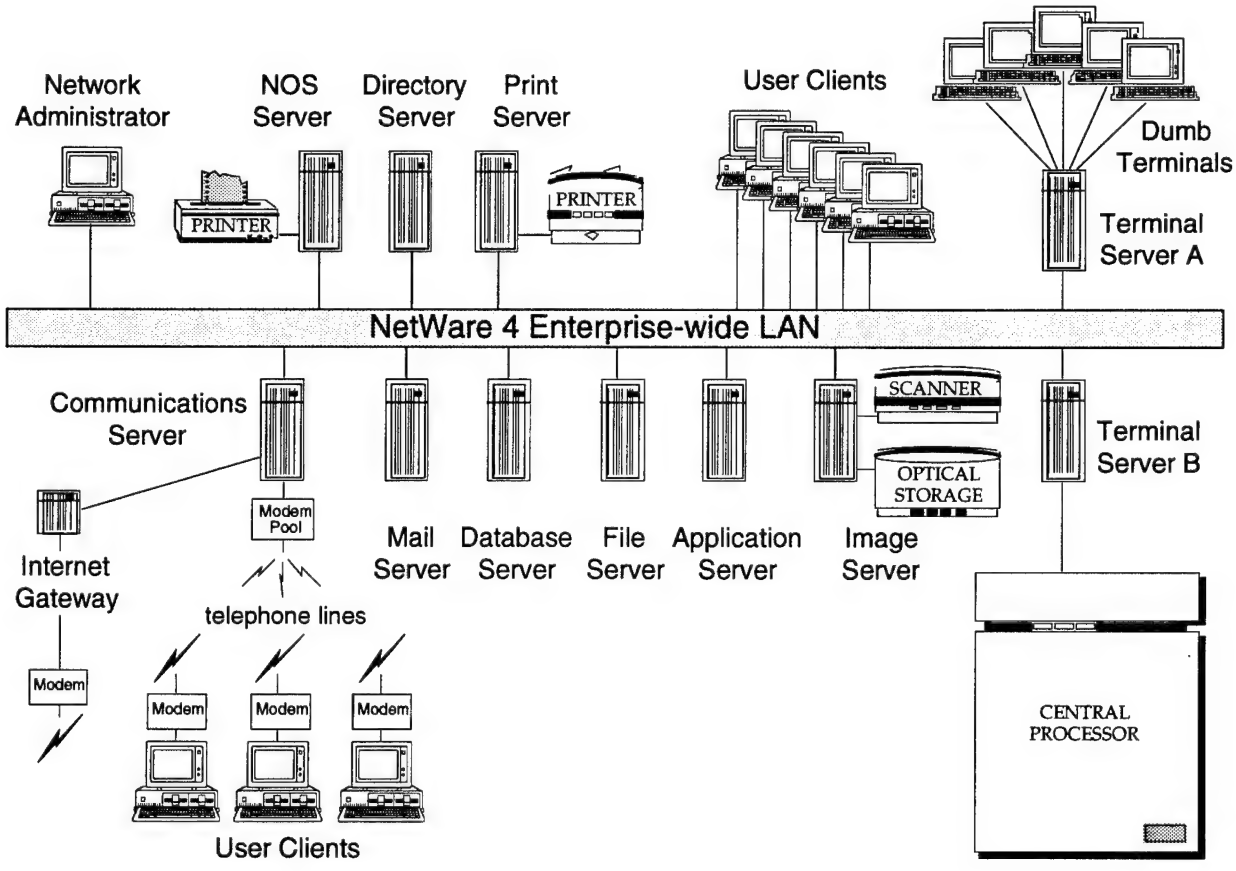


Figure 1-1. *A Robust Client-Server Environment*

platforms that are easy to customize for specific applications and provide magnitudes more processing power than the centralized systems they replace. In addition, they are scalable to meet current and future Naval needs.

With the centralized host model, management and security were relatively straightforward. Today, placing files and databases on dedicated servers has several of the advantages that were present in centralized systems: the centralization of data management facilitates the supervision and control of information; the servers are easier to secure and maintain because they are in one location managed by one authority; and backups are simplified for the same reasons. In fact, with fault tolerance and redundancy features, LANs can often provide a higher level of service assurance than can a mainframe. Fault tolerance and recovery capabilities are designed into many networks in order to minimize the risk of the network being unavailable and to maximize the speed of recovery when it is unavailable.

Approximately 60 percent of the network operating systems (NOSs) in operation today are Novell NetWare. Other major NOSs include AppleShare, Banyan's Vines, Artisoft's LANtastic, and Microsoft's recently introduced Windows NT. Novell NetWare was the first true file-server system available for PC LANs. NetWare runs on most PCs in either a DOS or Windows environment and supports DOS, OS/2, and Macintosh workstations. [DAVIS 94] A NetWare file server makes it possible for programs running on user workstations to locate and retrieve files from the server just as though the files were being retrieved from the workstation's local hard disk. To the application program, the files look and act just as they would if they were stored locally. Applications can also be located on NetWare servers for transparent access from workstations.

NetWare 2 and NetWare 3, originally designed to run on 80286 and 80386 hosts respectively, are server-centric. These versions have been upgraded to run on the 80486. NetWare 3 is currently the most widely installed version of NetWare. The management database for these versions of NetWare, called the *Bindery,* is specific to one server; that is, these versions are designed to operate on single dedicated servers. Each NetWare 2 and 3 server is managed individually because there is no management communication between servers. Thus, the NetWare Administrator has to establish access rules in the Bindery of each NetWare 2 and NetWare 3 server. Two objects (e.g., users, printers) cannot be assigned the same name because they would not be distinguishable.

Novell's most current version of NetWare is NetWare 4. With version 4, administrators view the network as a single entity – *an Enterprise Network* – rather than as a collection of individual servers, each needing individual management and control. With NetWare 4, references to objects include both the name and location. Thus, two users (or other objects) having the same name can exist on the network, or even on the same server. User accounts are set up once and are given appropriate access rights to any server on the network for which they are authorized. The NetWare 4 Administrator establishes access rules with one database for the entire network. This database is called *NetWare Directory Services (NDS).* Servers can be added or removed with minimal effort and access rules can be applied uniformly across the network.

Many organizations that have NetWare 3 installed are in the process of, or are contemplating, migration to NetWare 4. It may be necessary for NetWare 3 servers to exist in a NetWare 4 environment if applications which have not been upgraded to run under NetWare 4 are needed by the organization. In such cases, the administrator need only create the NetWare 4 enterprise-wide NDS database; NDS can emulate NetWare 3 binderies for the NetWare 3 servers.

Because of the large base of installed NetWare networks in both commercial and military organizations, there are many NetWare administrators in need of precise guidance on the administration of security in NetWare networks. Also because of this proliferation of NetWare installations, there is an abundance of documentation and reference manuals for NetWare. Experienced NetWare administrators will find many of the reference manuals extremely informative and useful. However, there is no single compact source devoted to security, particularly one that is focused on the less experienced administrator.

NetWare 4 includes many security features that the administrator should be aware of and implement. NetWare 4 includes new features that experienced NetWare 3 Administrators may not be aware of. Because NDS is complex, the administrator must take certain precautions in order to avoid unknowingly creating vulnerabilities in the security structure. In addition, there are many third-party products that can be installed to further enhance security in sensitive environments. Security issues concerning sensitive environments and the use of third-party products must be understood by first-time administrators in order to make intelligent decisions.

1.2 Scope

This handbook identifies the high-level security implementation requirements for sensitive environments and discusses NetWare 4 features that meet those requirements. *It is suggested that NetWare Administrators read this handbook while sitting at the NetWare console where they can log on as the NetWare Administrator in order to check and modify security settings.* Pointers to detailed references are included for the reader who wishes to investigate specialized topics of interest to a deeper level.

This handbook goes on to discuss additional security issues that are not solved by the implementation of NetWare 4 security features, and suggests third-party products that are available to help resolve some of those problems. Thirdly, this handbook discusses, in high-level terms, the issues concerning external interfaces since many organizations are faced with the decision of whether to connect to external networks or remain isolated in the interest of better security. Finally, this handbook attempts to surface security concerns that remain in spite of the installation of NetWare features and third-party products so that the security administrator can at least be aware of the concerns and be alert to changes that may elevate the importance of these issues.

1.3 Objectives

The objective of this handbook is to provide consolidated, concise, and easy to read security guidance on Novell NetWare so that the administrator will be able to take the correct steps to counter any threats that may arise. It is intended that all major security issues and topics be raised at a very high level to acquaint the new administrator with the issues. It is further intended that this handbook will provide guidance in each of those areas and pointers to more in-depth documentation on each subject.

This NetWare 4 Administrator's Security Guidance Handbook is intended for the inexperienced administrator who may not have a technical background with NetWare. The purpose is to facilitate consistent maintenance of NetWare network security during personnel turnover. The handbook is also intended for the experienced NetWare 3 Administrator who is responsible for migrating their organization's network to NetWare 4 but who has not attended NetWare 4 administration courses.

In addition, the handbook serves as a device for briefing management on security, resource, and funding needs. Managers and administrators can review this handbook in one day and absorb the basic concepts. Of course, much more time is needed to fully understand the recommendations and suggestions concerning NetWare security.

1.4 Report Organization

The main body of the report is organized as follows:

- **Section 1** – Introduction
- **Section 2** – NetWare 4 Security Features Implementation Guidance
- **Section 3** – Third Party Security Products
- **Section 4** – External Interfaces
- **Section 5** – Residual Vulnerabilities
- **Section 6** – Conclusions and Recommendations.

The following appendices are provided to supplement the main body:

- **Appendix A** – Acronyms
- **Appendix B** – Points of Contact and Other Resources
- **Appendix C** – Recommended Reading
- **Appendix D** – References.

Section 2

NetWare 4 Security Features Implementation Guidance

Secure Solutions, Inc.

Contract No. N00039-93-C-0099

This Page Intentionally Left Blank

2.0 NetWare 4 Security Features Implementation Guidance

In NetWare 3, security was based on the file server. In NetWare 4, security is based on the *object* (i.e., user or resource) and its location in the NetWare Directory Services (NDS) Directory tree. Thus, security is file server independent. Since security has been removed from the file server and placed into the logical map, NDS, the administrator now has much greater flexibility in providing object security.

NetWare 4 security involves controlling user logins, controlling access rights to the NDS Directory tree, and controlling access rights to the file system, including setting file attributes. Access rights are assigned in both the Directory tree and the file system. File attributes work with file system security to *inhibit* user access capabilities and enhance security. In addition, login controls are implemented when user accounts are activated. Of course, physical protection of servers and their consoles is always necessary, as is security of the printing services.

The first of the two major layers of security is implemented in NDS; the other in the file system. NDS is a special-purpose database which administers the security of resources, services, and user accounts. In other words, it is a logical map that allows users to locate and access resources (i.e., *objects*) anywhere in the network. NetWare Administrators are responsible for maintaining this logical map. The file system consists of volumes contained on the servers. Each volume has its own directory structure (not to be confused with the NDS Directory tree, indicated by a capital 'D'). NDS and the file system, shown in **Figure 2-1**, are separate, though closely related.

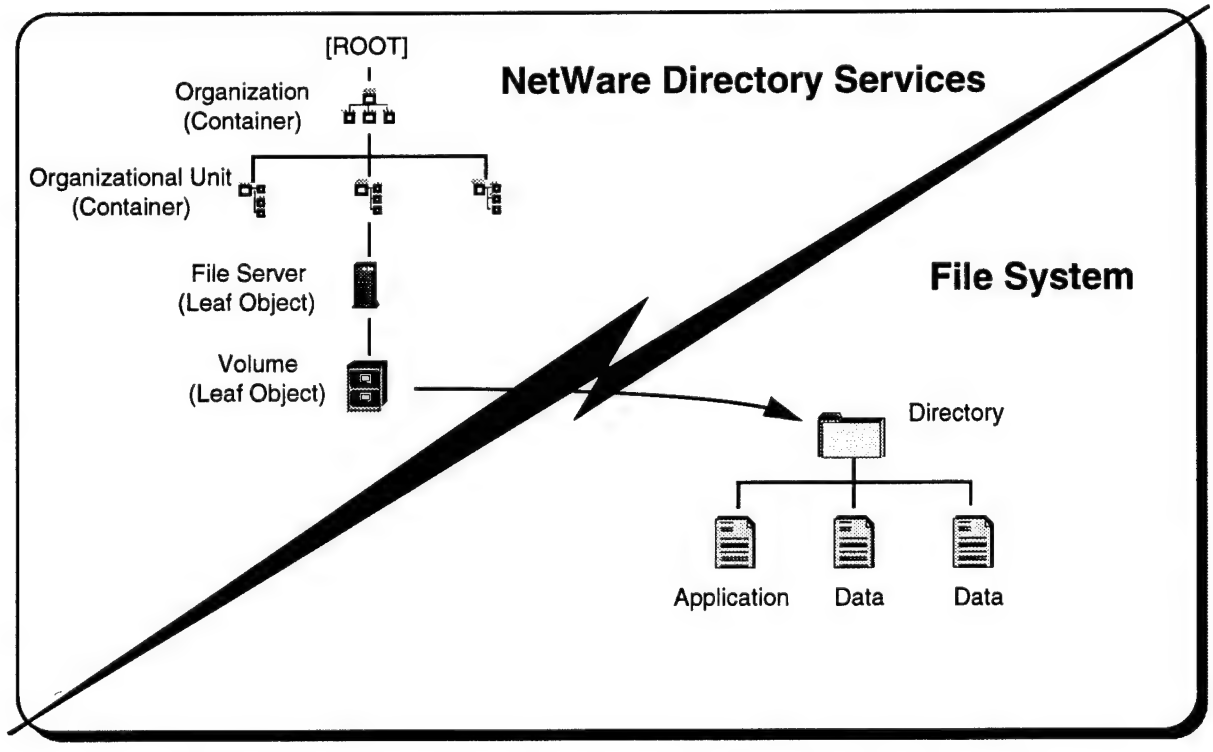


Figure 2-1. *Relationship Between NDS and the File System*

NetWare 4 includes two separate and distinct types of access rights: not surprisingly, NDS rights and file system rights. NDS rights control accesses to the Directory tree and, accordingly, to all the network resources, while file system rights control accesses to the data and software files. NDS does not control the NetWare file system, though it does control access to the server and volume objects where file system directories and files reside. Access rights to files are controlled by the NetWare file system. **Figure 2-2** depicts the NDS and file system trees.

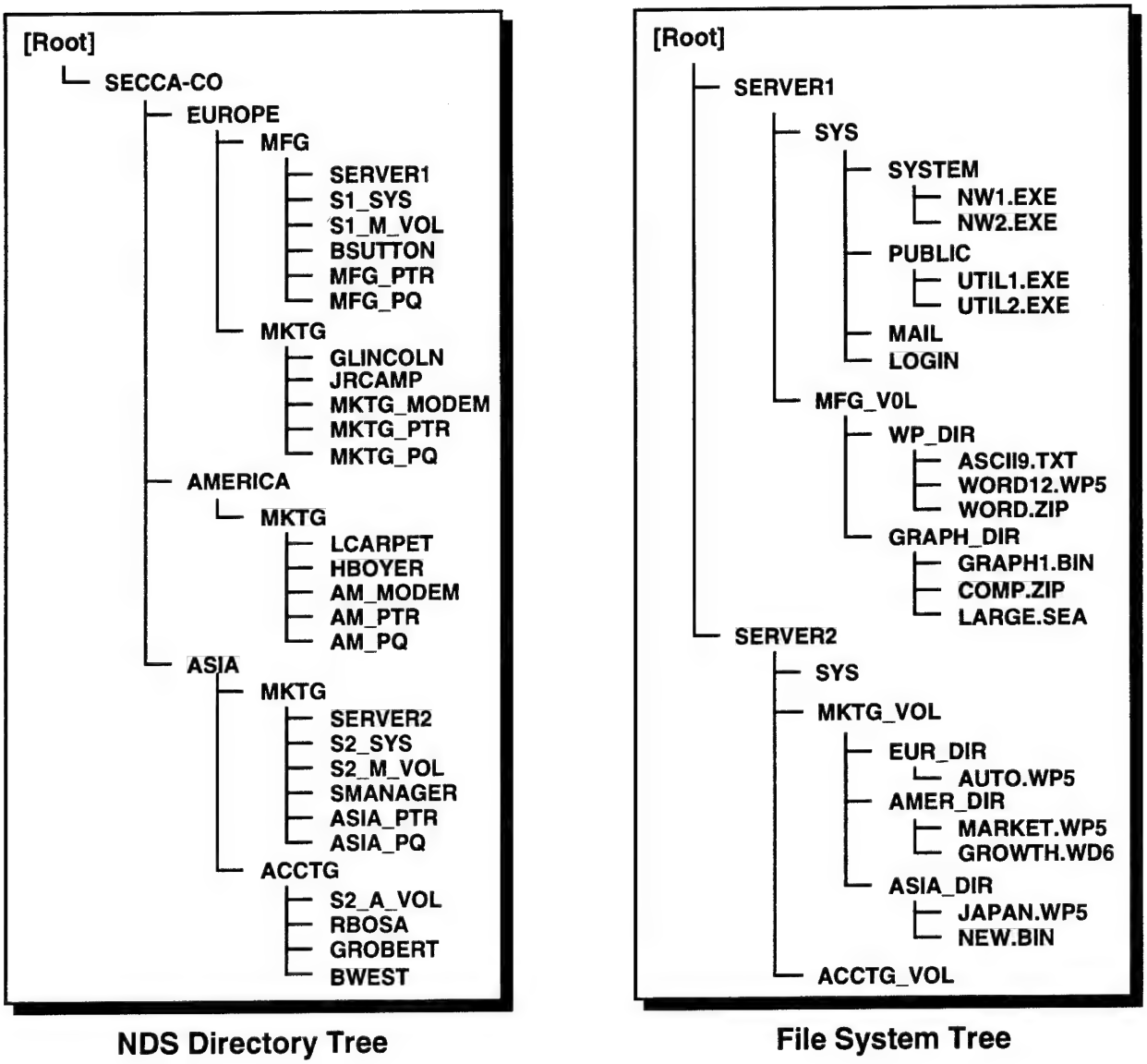


Figure 2-2. *Relationship Between the NDS and File System Trees*

The NetWare administrator is responsible for establishing and maintaining both Directory tree and file system security. In Windows and OS/2 environments, both can be managed with one utility, the Graphical NetWare Administrator (NWADMIN). In fact, NWADMIN can also be used to manage the printer environment. In a DOS environment, the administrator must use separate utilities to manage NDS and the file system: NETADMIN for NDS, and FLAG (a DOS character-mode utility with menus) and FILER (used to set attributes from the DOS command line) for the file system. While Macintosh clients are supported by NetWare and Macintoshes can be used as file servers, a Macintosh cannot be used to administer the network. (Note: Novell and Apple are working to develop the capability for a Macintosh to be used as a NetWare administrator's server.)

It is essential that the NetWare administrator understands the difference between NDS and the file system and knows how to set the various NetWare 4 rights correctly. A brief overview is provided below, though the NetWare administrator must acquire a much deeper understanding through Novell Certified NetWare Administrator (CNA) training or careful study of some of the suggested readings provided in **Appendix C**.

This section begins with a discussion of the Directory tree and file system, the rights that apply to each, file system attributes, and NetWare 3.X bindery emulation. Once NetWare structures and access rights are understood, the focus will turn to the user. The administration of user accounts will be discussed, followed by printer and print queue security, server console security, and monitoring and auditing. The section concludes with a short discussion of administrative issues including backup and recovery, authentication, and service assurance.

For additional high-level information on the structure and relationship between NDS and the file system, see [SHELDON 94]. For more information on the NetWare family tree (i.e., NetWare 2.X, 3.X, and 4.X) see [LAWREN 93]. Both of these references are described in **Appendix C**, Recommended Reading.

2.1 Directory Tree Security

The NDS database is designed as an inverted tree, known as the *Directory tree.* NDS database records, known as *objects*, store information about organizational units, called *container objects* (think of these as subdirectories, thought NDS actually has no directories or subdirectories), and network resources, called *leaf objects,* such as users, file servers, server volumes, computers, printers, print queues, and print servers. Novell icons for many of these objects, as well as those for NetWare mail (i.e., Message Handling System), are shown in **Figure 2-3**.

While the Directory tree is separate from the file system, one type of NDS object, called a "Directory Map", identifies a file system directory path. The purpose of a Directory Map is to facilitate easy access to frequently used applications and files without requiring the full path names to be entered each time access is desired. NDS

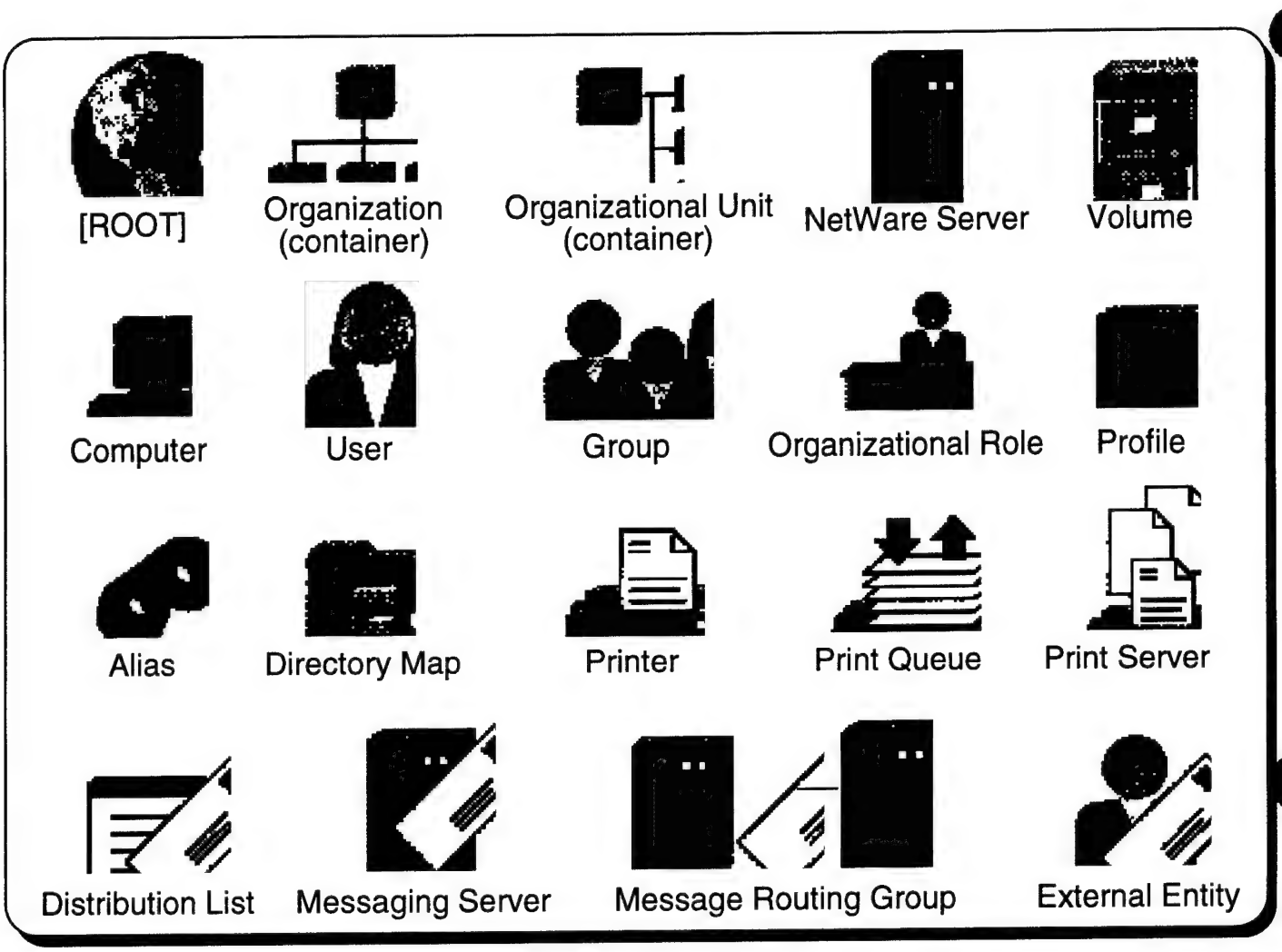


Figure 2-3. *NDS Container and Leaf Objects*

objects contain information, called *"properties"*, that describe users and network resources. Properties are fields assigned to an object; the values placed in the property fields are what actually describe the resource.

NDS provides two types of access rights: *object rights* and *property rights*. Object rights govern who can use the Directory tree to manage NDS objects (i.e., Directory tree records that describe user accounts and network resources). Property rights control who can change the property values in the NDS database. NDS rights are primarily given to NetWare administrators to create and manage network resources. Some NDS rights may be granted to users to manage portions of their own account, such as their login script.

An overview of NDS object and property rights is provided below. A brief discussion on planning NDS effective rights follows. Finally, recommendations on NDS security are provided. **Section 2.2** will discuss the File System.

For a complete listing of NDS and Bindery objects and properties, refer to the *NetWare 4 Network Computing Products: Utilities Reference* [NOVELL 94U].

2.1.1 NDS Object Rights

NDS object rights control what users with rights, called *trustees,* are allowed to do with NDS objects but do not allow access to the *properties* contained in the object. *Note: users become trustees when their User Objects are assigned to the Access Control List (ACL) of other NDS objects (e.g., containers, servers).* Object rights are shown in **Figure 2-4**.

Supervisor	Grants ALL object rights AND property rights.
Browse	Trustee can see the object in the directory tree.
Create	Applies only to container objects – allows the trustee to create a new object in the container object.
Delete	Delete an object (leaf or empty container) from the directory tree.
Rename	Change a leaf object's name.

Figure 2-4. *NDS Object Rights*

2.1.2 NDS Property Rights

NDS property rights control what *trustees* are allowed to do to the *properties* contained in the NDS database objects. Property values describe an object. For example, user account objects have the following properties: full name, common name, telephone numbers, e-mail address, street address, account balance, login restrictions and password requirements, and Security Equivalence List, discussed below. Resource objects have different properties such as: name, description, location, telephone number, and ACL. ACLs specify which trustees have rights to the object and its properties, and what rights they have. Many properties, such as mail lists, contain multiple values. Property rights are shown in **Figure 2-5**.

Supervisor	Grants ALL rights to an object's properties.
Compare	Allows the trustee to compare a value to the value of the property, but does not grant *Read* access to the value.
Read	Allows the trustee to see the value of a specified property. Automatically grants the *Compare* right.
Write	Add, remove, or change any value of a specified property. Automatically grants the *Add or Delete Self* right.
Add or Delete Self	Allows the trustee to add or remove itself as a value of the property. This is useful for properties such as group lists.

Figure 2-5. *NDS Property Rights*

2.1.3 Planning the Directory Tree and Effective Rights

The Access Control List (ACL), a property of an NDS object, can be used to explicitly define which other objects (i.e., trustees) can access the object and its properties. NDS object and property rights assigned in the upper levels of the Directory tree flow down the branches to container and leaf objects. This process, known as *inherited rights,* simplifies the task of rights assignments and management. NetWare gives the ability to block inheritance. It is done with an Inherited Rights Filter (IRF). Rights will continue to flow down until they are blocked by an IRF. If a container has an IRF, an object in that container can only inherit rights from above the container that are specified in the IRF. Any other rights are blocked from flowing down the tree. Furthermore, the IRF cannot be used to assign rights; rights assignments are done in the ACL by defining objects as trustees. Trustee assignments can be made at any level. **Figure 2-6** shows an example where NDS object rights are inherited from container objects above. The SECCA-CO container object inherits the browse right to NDS objects. Rights are reassigned using a trustee assignment at the EUROPE level and blocked using an IRF at the MKTG level. The rename right is inherited by the GLINCOLN leaf object since there is no IRF to block it.

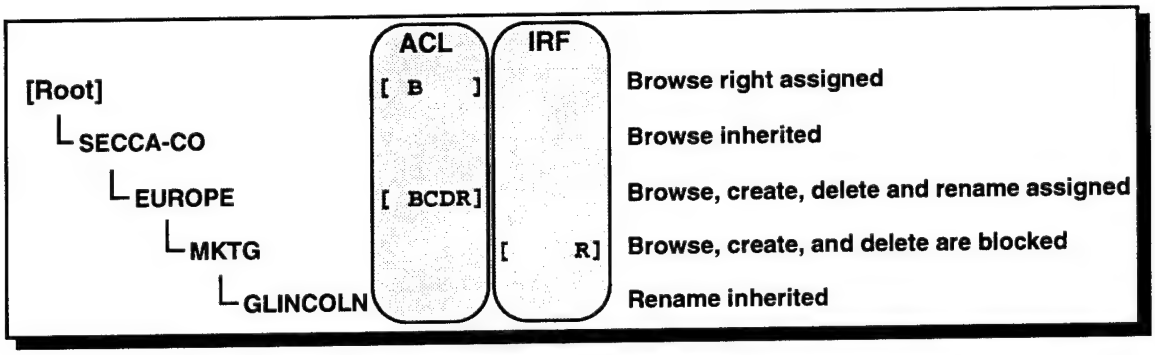


Figure 2-6. *Inherited Rights Filter (IRF) Used with NDS Object Rights*

NDS property rights are inherited in the same manner: through trustee assignments to containers above and through IRFs that block rights from above. However, there is an *important* exception. When property rights are assigned to an object using the All Rights option, they flow down, but when rights are selectively assigned to properties of an object, they do not flow down.

In addition to controlling how objects inherit rights, the NetWare administrator can assign *security equivalence* which assigns the rights of one object (often a User, Organizational Role, or Group) to another object on the network. This is accomplishing by adding an object with rights to the Security Equivalence List of the object receiving the rights. Security Equivalences are difficult to track and its use is not recommended.

It is important to plan the effective rights of all objects in the Directory tree. The administrator must consider what rights will be assigned at the various levels of the tree, what rights will be filtered using Inherited Rights Filters, and what rights will be permitted

to be inherited. An ACL can be used to explicitly define trustees for an object and its properties. Security Equivalences can be defined to assign additional rights to objects, though this is not recommended. The preferred approach is to assign rights to groups and then place objects in the groups. With proper planning, the entire process can be streamlined so that rights can be assigned and changed quickly and efficiently.

For more information on the Access Control List, Inherited Rights Filter, and effective rights, review [NOVELL 94R] and [HEBRON 94].

2.1.4 Important NDS Recommendations

When planning the Directory tree, look at the organization chart and determine who reports to whom and where servers, printers, and other resources physically reside. Standardize the naming conventions for the entire organization prior to installing NetWare. A standard technique for assigning names to Organizational Units, Servers, Volumes, Users, Printers, Queues, Organizational Roles, and other NDS objects should be implemented. This is particularly important before migrating NetWare 3.X servers to an enterprise-wide NetWare 4.X so that there are no naming conflicts.

When deciding where to place User objects in the Directory tree, try to combine User objects into the same container object if they share the same applications, file server, and printers. For example, personnel from the same department are good candidates for placement in the same container, which would be named after the department. Combining objects also helps to reduce the traffic on the network by making servers and printers available locally to the users that use them the most.

To streamline creation of User objects within a container and to provide commonality of properties (address, phone, and other repetitive fields), establish a User_Template with the desired basic information. Whenever a new user is created in the container, the User_Template can be copied to the new User object. The User object's properties can then be tailored. Often, it is best not to assign rights to User objects. If the User objects in the container are not all going to have the same rights, Novell recommends that User objects be assigned to Groups and then the Group objects be assigned rights. This avoids the explicit assignment of rights to every User object in the Directory tree. Users should only be made trustees of their individual home directories.

If all users in a container are to receive the same rights, an even better way to control access than assigning rights to groups is to assign them to containers so they are inherited by all User objects placed in the containers. That way, when a user is moved to another container, they automatically lose the old rights and have the new rights. They can still be made members of groups for access to objects that other users in the container do not need (such as applications and databases used by another department). A word of warning, though: if the container (for example, an Organization) has Supervisor right to the server, all User objects inside the container have Supervisor right to the server. So while this is a powerful way to administer rights, it requires skill and caution.

- Plan Directory tree and naming conventions
- Use the default rights delivered with NetWare to the extent possible
- Combine User objects that share resources into one container
- Copy User_Template when creating User objects
- Avoid assigning rights to individual User objects
- If various rights are needed, assign users to Groups and give rights to the Group
- Assign rights to the container when all users will have the same rights
- Use Organizational Role to create container administrators
- Use Security Equivalence only to assign temporary rights
- Avoid assigning property rights with the All Properties option
- Never give WRITE property right to All Properties of a container
- Never grant SUPERVISOR right to a Server object
- Container administrators should not block SUPERVISOR right to containers
- Subordinate administrators should not block SUPERVISOR right to servers
- Use Alias objects to grant users access to resources outside their context
- Consider removing BROWSE right from [PUBLIC]

Figure 2-7. *Summary of NDS Recommendations*

Alias objects are objects that point to actual objects in other containers in the Directory tree. Alias objects are a useful tool for granting rights to users that frequently have a need to operate outside their normal context (i.e., outside the container where their User object's resides in the NDS Directory tree). Users who often log in from workstations with a different default context from where they need to be can be assigned Alias objects. Similarly, a printer that is shared by two departments (and thus, two containers) can be assigned an Alias. The Printer object can be accessed by users in the same container, and the Printer Alias object can be accessed by users in the container where the Alias is located.

Selective use of Organizational Role objects, security equivalences, and ACL trustee assignments also helps to streamline the rights assignment effort but must be planned carefully. Security equivalence assignments should only be used to assign temporary rights to users. Furthermore, *the use of Security Equivalence to give administrator rights to an alternate administrator should be avoided* because if the original user object is removed, the alternate administrator will lose their rights as well. In addition, the alternate may have more access than is needed. Instead, it is recommended that container administrators be created using the Organizational Role object and multiple

occupants assigned to the Role. A second administrator could be set up as a "back door" for use in emergencies. In this case, put the password in a sealed envelope and store the envelope in a safe where it cannot be compromised.

As a general rule, always grant as few rights as possible and add rights when users demonstrate a need for greater access. NetWare is delivered with default rights assigned in NDS. Do not modify these without understanding the repercussions.

Rights granted to [PUBLIC], a special trustee, are passed to everything attached to the network. This includes users that are connected, but not yet authenticated and logged into NetWare. Typically, the [PUBLIC] trustee should only have the Browse object right and Compare and Read property rights. But even this has some risk associated with it. The CX command allows users to see their current context. The CX command with the /T/A options will show the entire NDS Directory tree if [PUBLIC] has the Browse right. The assignment of [PUBLIC] as a trustee of containers (especially [ROOT]) should only be done after careful consideration of less powerful approaches for granting access. If this cannot be avoided, consider manually removing the Browse right from [PUBLIC] to prevent outsiders from browsing the NDS Directory tree and seeing what users and network resources exist. If this cannot be done, as is often the case, at least be aware of the risk.

Do not give Write property right to a container when *All Properties* is selected because that gives User objects in the container the Write capabilities to the ACL property and they can add themselves as trustees of the container, giving themselves the Supervisor right. If a trustee is granted the Write property right to an object, the right should be granted only to selected properties that the trustee is allowed to change, such as the login script, postal address, and phone number, *and not to the ACL property.* In other words, Write privilege to All Properties is the same as giving the trustee Supervisor privileges to the object (this applies to a both container objects and leaf objects). In fact, avoid assigning any property rights through the use of the *All Properties* option because many object properties contain private information that should be protected.

If the Supervisor right is granted to an NDS Server object, then the Supervisor right will flow to the file system for every volume attached to that server. *Therefore, do not accidentally grant Supervisor rights to any NDS Server object!* Furthermore, granting Write property right to the ACL property will do the same thing. *Therefore, do not grant Write access to the Server object ACL property.*

A warning to subordinate managers: when blocking the Supervisor right to the NDS Server object (or any other object), be careful not to make a branch of the Directory tree unreachable by the administrator. This might occur if the NetWare administrator makes a department manager the administrator of a container, and the department manager then installs an Inherited Rights Filter (IRF) to block the NetWare administrator's Supervisor right to the container. At a later date, the NetWare administrator deletes the User object for the department manager leaving nobody with Supervisor right to the container!

In summary, there are seven ways users can be given rights to NDS objects:

- [ROOT] rights
- [PUBLIC] trustee rights
- Inherited from parent container (or higher)
- Group assignments
- Organizational Role assignments
- Security Equivalence assignments
- Explicit trustee assignments.

All of this becomes relatively straightforward with training, practice, and prior planning. The use of IRFs, User_Templates, Aliases, Groups, Organizational Roles, and security equivalences simplify the process after the structures are initially set up.

2.2 File System Security

The file system is managed independently of the NDS Directory tree. File system concepts are more familiar to most administrators since they are similar to the structures used in DOS. Therefore, setting up the file system should be more straightforward that setting up the NDS Directory tree.

Where NDS trustees have up to five object rights `[SUPERVISOR BROWSE CREATE DELETE RENAME]` and five property rights `[SUPERVISOR COMPARE READ WRITE ADD-OR-DELETE-SELF]` for access to NDS Directory objects, the file system provides up to eight rights for access to directories and files `[SUPERVISOR READ WRITE CREATE ERASE MODIFY FILE-SCAN ACCESS-CONTROL]`. As with the NDS Directory tree, rights flow down the branches of the file system tree and can be blocked using an Inherited Rights Filter (IRF). A key difference though, is the fact that Supervisor right cannot be blocked in the file system (remember that Supervisor right can be blocked in NDS and the risk is that a branch of the Directory tree could become unmanageable!). This means that the administrator can always access and backup every directory and file in the file system.

The file system also allows the assignment of *attributes* to directories and files which dictate what can be done with them. Attributes work with trustee rights to inhibit user access capabilities and enhance security. For example, a user may be assigned as a trustee of a file and be given the WRITE right, but if the READ-ONLY attribute is set for the file, that user cannot write to it! *Warning: the Modify right gives the trustee the ability to change attributes, such as the READ-ONLY attribute, and defeat their protection.*

This section reviews file system rights and attributes, discusses how effective rights are calculated, and offers recommendations for administration of the file system. For additional high-level information on the file system, see [NOVELL 94R]. For detailed information on administration of the file system, see [NOVELL 94S].

2.2.1 File System Rights

Users need different levels of access to the file system. A user should be able to create and delete files in their personal directory as if the files were on their PC's hard disk, but they should not be able to modify application programs and they should be denied all access to many of the files belonging to other users. The NetWare **file system directory rights** control what users, called *directory trustees,* are allowed to do with file system directories but do not allow access to the *attributes* contained in the directories. The NetWare **file system file rights** control trustee accesses to the files. File system directory and file rights, written as [SRWCEMFA], are shown in **Figure 2-8**. Note that CREATE right normally applies only to directories, and not to files. However, trustees can only recover a deleted file using the FILER utility if they have the CREATE right to the file that has been deleted.

For additional information on the assignment of file system rights, see [LAWREN 93]. For detailed information on file system rights, see [NOVELL 94S].

	DIRECTORY RIGHTS	FILE RIGHTS
Supervisor	Trustee has ALL rights to the directory and subdirectories. This overrides IRFs for the directory and subdirectories.	Trustee has ALL rights to the file, can change the file's IRF, and can give other users the SUPERVISOR right to the file.
Read	Trustee can read the contents of existing files in the directory.	Trustee can read the contents of the file.
Write	Trustee can change the contents of existing files in the directory.	Trustee can change the contents of the file.
Create	Trustee can create a file or subdirectory in the directory.	Trustee can recover a deleted file using the FILER Utility.
Erase	Trustee can remove a file or subdirectory from the directory.	Trustee can erase the file.
Modify	Trustee can rename files and subdirectory in the directory or change their attributes.	Trustee can rename the file or change the attributes of the file.
File Scan	Trustee can list the files in the directory.	Trustee can list the file even without FILE SCAN right for the directory.
Access Control	Trustee can give other users rights to the directory and to modify the directory's IRF.	Trustee can give other users rights to the file and to modify the file's IRF.

Figure 2-8. *File System Rights*

2.2.2 File System Attributes

Attributes can be assigned to both directories and files. Attributes override rights. Directory and file attributes are shown in **Figure 2-9**.

	DIRECTORY ATTRIBUTES	FILE ATTRIBUTES
Archive	–	File has been changed since last backup.
Copy Inhibit	–	Macintosh users cannot copy file.
Delete Inhibit	Even users with ERASE right cannot delete directory. (But they can delete files in it.)	Even users with ERASE right cannot delete file.
Don't Compress	Files in directory will not be compressed.	File will never be compressed.
Don't Migrate	Directory will never be migrated.	File will never be migrated.
Execute Only	–	Applies only to executable files – (.EXE or .COM) – cannot copy file.
Hidden	Directory is invisible to DOS commands.	Programs cannot list, copy, or delete file.
Immediate Compress	Files in directory will be compressed as soon as possible.	File will be compressed as soon as possible (overrides waiting period).
Purge	Purge immediately upon delete. (Makes delete permanent)	Purge immediately upon delete. (Makes delete permanent)
Read Only	–	File cannot be modified or deleted.
Rename Inhibit	Directory cannot be renamed.	Even users with MODIFY right cannot rename this file.
Shareable	–	File can be accessed simultaneously by multiple users.
System	Directory is for system use only; invisible to all others.	File cannot be listed by programs. (Used for two specific DOS files.)
Transactional	–	Used with Transaction Tracking System (TTS) – updates made only when transaction completes.

Note: DOS only supports attributes that are underlined. Thus, they can be supported on the PCs hard disk or the file server. Others are only supported on the file server.

Figure 2-9. *File System Directory and File Attributes*

2.2.3 Planning NetWare File System Effective Rights

The NWADMIN and FILER utilities and the RIGHTS command can be used to examine and modify the effective rights of a directory or file. The NDIR command can also be used to view file system rights. Several factors decide the effective rights:

- Trustee rights to the parent directories
- IRF of the directory
- Trustee rights to the directory
- IRF of the file
- File attributes.

If there is no IRF or trustee rights assigned to the directory, then the rights assigned to the parent directory are inherited. This greatly simplifies the task of assigning trustee rights. If the current directory has an IRF, then only the rights in the IRF can be inherited. (The only exception is that SUPERVISOR rights cannot be blocked in the file system. If SUPERVISOR is an effective right in the parent directory, it will be inherited regardless of the IRF.) Furthermore, the IRF cannot add rights. It only specifies what inherited rights will be blocked.

If unique trustee rights are assigned, they are added to the inherited rights. For example, if the IRF blocks all but SUPERVISOR, READ, and FILE SCAN [SR F] to a directory and READ [R] is inherited, and the unique trustee has WRITE, CREATE, ERASE, and FILE SCAN [WCE F] rights for the directory, the effective rights are [RWCE F]. The same would be true for a file.

Parent directory effective rights	[RWCEM]
Directory IRF	[SR F]
Directory inherited rights	[R]
Directory trustee rights	[WCE F]
Directory effective rights	[RWCE F]

The file's IRF determines which rights the file can inherit from its directory. If a file has an IRF of READ and FILE SCAN [R F] but no trustee rights are added, the IRF will prevail even if READ, WRITE, CREATE, ERASE, AND FILE SCAN [RWCE F] trustee rights had been assigned to the directory above. Therefore, the effective rights to the file would be [R F].

Directory effective rights	[RWCE F]
File IRF	[R F]
File inherited rights	[R F]
No file trustee rights	
File effective rights	[R F]

File *attributes* prohibit the use of rights. For example, if a trustee has effective rights of READ, WRITE, CREATE, ERASE, and FILE SCAN, but the READ ONLY (Ro) attribute is assigned to the file, the user can only read the file.

File effective rights	[RWCE F]	
File attributers	[Ro]	<— only Ro access permitted

2.2.4 Important File System Recommendations

Since the structure of the file system is well known, not many recommendations are necessary. The most important recommendations associated with the file system actually pertain to NDS. As discussed under NDS, if the Supervisor right is granted to an NDS Server object, then the Supervisor right will flow to the file system for every volume attached to that server. *Therefore, do not accidentally grant Supervisor rights to any NDS Server object!* Furthermore, granting Write property right to the ACL property will do the same thing. *Therefore, do not grant Write access to the Server object ACL property.*

Also discussed under NDS security, Rights granted to [PUBLIC], a special trustee, are passed to everything and everyone attached to the network. To be *attached* means to be connected to a server but not necessarily authenticated yet, and thus not yet logged into NetWare. The assignment of [PUBLIC] as a trustee of file system directories and files will make those directories and files accessible to outsiders. Do not make [PUBLIC] a trustee of sensitive directories or files.

Another file system recommendation is to avoid using Inherited Rights Filters to block rights. Instead, redesign the rights at the upper levels so that the rights structure is as simple as possible.

The CREATE right is not normally associated with files, only directories. The NetWare administrator may want to assign CREATE rights for files so that files which are inadvertently deleted can be recovered using the FILER Utility.

2.3 NetWare 3.X Bindery Emulation

The bindery is a database on NetWare 2.X and 3.X server that holds security and accounting information (just as NDS holds security and accounting information for NetWare 4.X servers). Bindery emulation is necessary whenever the network is running both NetWare 4.X and earlier servers, as is the case when applications developed for earlier versions of NetWare have not been migrated to run under NetWare 4.X. Bindery emulation allows NetWare 4.X servers to emulate Bindery mode for users who are running the NetWare 2.X or 3.X workstation shell instead of the NetWare DOS Requester used for NetWare 4.X. Also, older applications may not be NDS compliant. Bindery emulation will allow these applications to function within NetWare 4.

2.4 Administration of User Accounts

Simplicity and consistency are important when establishing user accounts. When the NDS Directory tree is being designed, User objects should be co-located into containers. Remember, any rights assigned to the container will flow down to all the User objects; if the container has Supervisor right to the server, all User objects inside the container have Supervisor right to the server. In a small organization, all users can be placed in one container. This allows the use of container login scripts (discussed below) for all users in the container and the setting of Intruder Detection and Lockout for the entire container.

The file system may also be easier to administer if user directories are colocated into one directory named \USERS. This make it easier for the administrator to locate specific user files and also facilitates the creation of backups.

In organizations with more than 50 users, it is recommended that a container for each site, division, or other sub-organization level be established. A naming convention should be followed so that it is easy to locate user accounts. Most accounts should be identified by the user's last name and first initial. Some user accounts will be required to continue to exist as personnel turnover occurs. These should be established as Organizational Role objects and be identified by job function such as DATABASE_MGR.

Disk space restrictions, called *volume restrictions,* should be assigned to user accounts using NWADMIN (Windows or OS/2 environments) or NETADMIN (DOS environments) so that the users are not able to act as black holes, sucking in every file they can find and preventing other users from having enough disk space. The amount of disk space required varies greatly depending on the applications to be used and the number and size of database records and files they expect to store in their personal address space. First try to determine what the users feel they need. Application manuals sometimes specify storage requirements. A reasonable estimate for user space would be in the 4MB to 20MB range depending on whether users will store text or graphics files, or whether they will be permitted to store applications for their private use. If no reasonable estimate can be determined, then begin by allocating 15MB of storage to each user. With the proliferation of multimedia applications, this allocation may have to be expanded within one or two years. This can be adjusted upward if the storage system is able to support larger accounts.

A negative consequence of implementing volume restrictions is that if a user has filled their workspace, they may not be able to print a document (since space is needed temporarily to create the print image) or even to save their file after a long period of work! It may be better to avoid these consequences by not implementing volume restrictions. If the NetWare administrator chooses this route, then a policy on disk usage must be established and disseminated to all users. Then the administrator must check that users are staying within the limits and must take action whenever a user repeatedly violates the limits. This course may be more difficult, but cause less social reaction.

- Co-locate Users that share resources into one container
- Assign Organizational Role objects as trustees for positions with high turnover
- Implement Volume Restrictions to limit the size of user workspaces
- Implement user account restrictions:
  - Login restrictions
  - Password restrictions
  - Network address restrictions
  - Time restrictions
- Establish User_Template for assigning object and property rights to users
- Install Map Drive and Search Drive pointers in Login Scripts
- Search for unauthorized executables in user directories weekly

Figure 2-10. *Summary of User Account Recommendations*

User account restrictions should be established in most Navy environments. The NetWare Administrator can use NWADMIN or NETADMIN to set login restrictions, password restrictions, network address restrictions, and time restrictions. *Login restrictions* include disabling accounts when personnel are on leave or TDY, setting account expiration dates which automatically disable accounts but do not remove them, and controlling concurrent connections (i.e., the number of workstations the user can login to simultaneously). *Password restrictions* include whether a password is required, whether the administrator or the user sets the password (user responsibility is recommended), minimum password length (six characters are recommended), lifetime limits for passwords (varies with sensitivity of the system), whether passwords can be reused (recommend preventing reuse for at least eight cycles), and whether grace logins are permitted after a password expires (recommend three grace logins). *Network address restrictions* control which workstations can be used by a particular user. This is especially important for some privileged accounts like DATABASE_MGR, but not necessarily for all users. *Time restrictions* allow the administrator to block logins during off-hours. This is one of the least used restrictions that is available for more sensitive environments. Time restrictions can be used by organizations with Internet connectivity to allow outsiders to login as Guest or Anonymous after normal working hours but to prevent the extra load during working hours. Third party products are available which automatically logoff inactive terminals (see NetSentry in **Section 3.4**, Network Analysis and Management). NetWare administrators in sensitive environments are advised to install such products since users who are not security conscious commonly leave active terminals unattended.

NetWare administrators are advised to establish a USER_TEMPLATE for each container with all the restrictions set and them copy that template to user accounts as they are created. This will simplify the process.

Drive mappings are necessary because DOS does not recognize NetWare directory paths, so pointers must be created and inserted into the DOS PATH statement. There are two types of drive pointers: Map Drives which point to user areas, and Search Drives which point to applications and shared databases. Map Drive pointers should be updated when the user enters a Change Directory (CD) command so that the user will return to the same subdirectory when returning from other drive pointers (i.e., changing from drive pointer F: to H: and back to F: should put the user back in the same subdirectory of F: rather than the initial entry point at the top of the directory). However, use of CD can be disastrous when the current drive is a Search Drive. Search Drive pointers are not intended to be dynamic since they point to applications and should always place the user at the application's main directory. Use of the NetWare MAP utility for mapping drive paths is tricky and can result in unexpected changes to Search Drive pointers without warning. Study NetWare documentation carefully before using the MAP utility and understand the differences between Map Drives and Search Drives. When assigning drive pointers, be sure to use the *root* option to prevent the user from exiting the subdirectory and ascending higher in the file system tree.

In many situations the NetWare administrator may choose to remap local drives (A: and B:) on workstations away from the floppy diskette drives in order to inhibit users from loading unauthorized software (though this can be defeated by experienced users). Drive mappings are stored in RAM and lost when the workstation shuts down. Remapping of drives is done by inserting appropriate MAP commands in the Container and Profile Login Scripts installed in user accounts that are automatically executed upon startup. Login scripts perform repetitive login functions when the user logs into the network, similar to what AUTOEXEC.BAT does when the user starts up their PC. There are four classes of login scripts that can be executed sequentially, as shown in **Figure 2-11**. *Container login scripts,* which are properties of container objects (Organization or Organizational Unit), and *profile login scripts,* which are properties of Profile objects, execute first and can only be modified by trustees with Write privilege to the Login Script property of the container and Profile objects (i.e., the administrator). *User login scripts* execute third and can be modified by the individual user. Container login scripts, profile login scripts, and user login scripts can be installed using NWADMIN or NETADMIN.

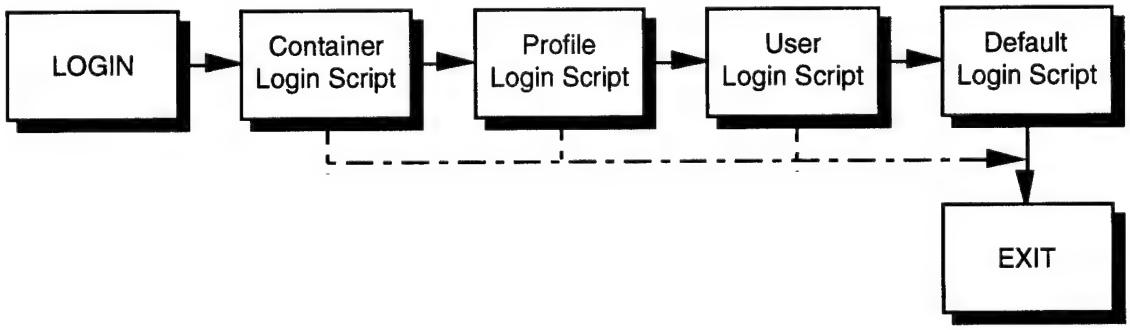


Figure 2-11. *Login Scripts*

The Default script is not modifiable, but can be bypassed by including "EXIT" as the last line of any of the previous three login scripts or by using "NO_DEFAULT" in any of the previous scripts. Similarly, by including "EXIT" in the container or profile login scripts, the users can be prevented from executing a user login script. This is recommended for some environments so that users are not able to create and execute custom login scripts.

Login scripts are useful in displaying network information, mapping drives (e.g., G: drive) to network directories (e.g., the user's home directory or a directory for an application), and capturing printer port output and redirecting it to a network queue. Several MAP and CAPTURE commands, as well as some other commands (there are 30), are generally repeated each time the workstation is powered up and logged onto the network. Drive mappings should reference Directory Map Objects (a *name* which is equated to a path) instead of the actual application path because there are times when applications may have to be moved to new servers. By using Directory Map Objects in login scripts, the administrator need only modify the Directory Map Object path in the NDS database when the application is moved. All login scripts that reference the object name remain unchanged.

One other useful indirection technique is the use of the INCLUDE login script command. Login scripts could have the INCLUDE command point to an external file that the administrator controls. That file can contain standard login script commands. When the administrator wishes to modify all login scripts, it can be accomplished simply by modifying the external file.

Other entries that are recommended in the container or profile login script are those that prevent the user from using [CTRL]-C to break out of the login script, and those that greet the user during login to notify them of their workstation connection number, last login, daily message, password expiration, and any recurring notices. For example:

```
BREAK OFF
WRITE "You have logged in from station %STATION"
WRITE "Your last login was at %LASTLOGINTIME"

DISPLAY S1_SYS:ADMIN\MESSAGE.TXT
REMARK - Administrator text-of-the-day in message.txt will be displayed

IF %PASSWORD_EXPIRES<="14" THEN
   WRITE "Your password expires in %PASSWORD_EXPIRES days."
END

IF DAY_OF_WEEK="FRIDAY" THEN
   WRITE "Be sure to purge your directory today.  Like the company "
   WRITE "refrigerator, if it is left here tonight, it will be gone Monday."
   REMARK - or other notice that should be displayed every Friday
END

SET PROMPT="$P$G"
EXIT
```

Returning to the discussion of remapping A: and B: drives away from local drives, there are several options that can be taken to help enforce the mapping. One option is for the administrator to remove the MAP capability from the user (from both the User Login Scripts and direct use) by moving the MAP executable from the [PUBLIC] directory (a special trustee that gives rights to all users attached to the network) and placing it in an administrator-only directory so the users cannot map drives A: and B: back to the local drives. In such environments, there may be times when the user requires the ability to use their diskette drives. During these times, the administrator should prevent the user from accessing the local C: hard drive or the network (by remapping their pointers to safe locations) until the local diskette drives are again disabled. Note: The NETWORK DRIVES option of FILEMGR in Windows can be used by users to restore or tamper with drive mappings without using the MAP command.

A second option which allows MAP to remain in [PUBLIC] would be to remove Windows from the individual workstations and run it on the network, then remove the file menu from it so the user cannot exit Windows and get to DOS. Restrictions would have to be set in PROGMAN.INI. This becomes very complex and may not be something the inexperienced administrator should pursue.

In a hostile environment, the only absolute way to prevent the loading of unauthorized software is to provide users with diskless workstations that have boot proms installed. This is a drastic measure. The recommended solution over this or other solutions discussed above is to establish a policy that prohibits the loading of unauthorized software and then enforce the policy. The NetWare administrator should create a batch file to search for unauthorized executables in the \USERS directory in the file system and run that file weekly. The following example would identify violations:

```
NDIR *.exe /sub
NDIR *.com /sub
```

In summary, the use of Organizational Role objects, User_Templates, and login scripts will simplify the process of managing user accounts. More importantly, they will make many NetWare features transparent to the user and thus easier to use.

For additional information on the administration of user accounts, see [LAWREN 93], [SHELDON 94], [NOVELL 94S], and [NOVELL 94V].

2.5 Printer and Print Queue Security

Local decisions must be made on where to attach printers to the network. Attaching printers to servers provides greater assurance of reliability and integrity, but attaching printers to workstations in the user areas provide greater flexibility and accessibility. Before considering security issues, a review of NetWare utilities and NLMs is in order since the many utilities related to printing can be confusing. The steps for setting up a print environment are:

1. Use NWADMIN or PCONSOLE to create: Print Queues, Print Servers, Printers. When finished, use NWADMIN to print the NDS Directory tree showing all objects (including print objects) in the tree

2. Load PSERVER.NLM on the server where the Print Server will reside. PSERVER is used to manage printers and print queues and generate audit logs

3. Load NPRINTER.NLM on servers (NPRINTER.EXE on workstations) where printers will be attached

4. (Optional) Use PRINTDEF or PRINTCON to set a container's *print job configuration.* (It defines printer name, print queue name, number of copies, banner, and printer form for print jobs to simplify the use of CAPTURE, NPRINT, PCONSOLE, and USER TOOLS.) *Note: this capability is included for completeness to show the administrator what the utilities are used for; it's use is complex and is not recommended. Today's software comes with print engines which eliminate the need for the administrator to set print job configurations.*

5. (Optional) Use NWADMIN or PRINTDEF to configure *printer forms*

6. Use NWADMIN or PCONSOLE to manage: Print Queues, Print Servers, Printers

7. Use CAPTURE command (either directly or in login scripts) or USER TOOLS (NETUSER) to automatically redirect output to network printers

8. Use NPRINT outside applications to direct print jobs to network printers.

Before attaching printers to the network, make sure they work in non-network environments. Consider the capabilities shown in **Table 2-1** when assigning print server and print queue operators, print server and print queue users, and the printer notify lists. Be sure to include passwords when creating NDS Print Server objects. Physically place printers in secure locations, particularly if the output may be sensitive, and consult your local Security Manual on policy concerning bannering and distribution.

For additional information on print services, see [NOVELL 94T] and [NOVELL 94U]. Another source that was written for NetWare 3.12 but is easy to understand and is still relevant in a NetWare 4 environment is [WILCOX 94].

LEGEND:
PS = Print Server
PQ = Print Queue

Capabilities	Supervisor	Print Server Operators	Print Queue Operators	Print Server User List	Printer Notify List	Print Queue User List	Other NetWare Users
Create/delete PS, PQ, Printer objects	✓						
Modify PS and PQ Operator List	✓						
Modify PS and PQ User List	✓	✓					
Assign PQ to Printer	✓	✓					
Modify Printer Notify List	✓	✓					
Shut down PS		✓					
Modify Printer status		✓					
Modify PQ operator flags			✓				
Manipulate other's print jobs in PQ			✓				
Monitor PS	✓			✓			
Receive Printer error messages				✓	✓		
Print job owner						✓	
Send print jobs to PQ						✓	
Use PQ						✓	
Manipulate own print job in PQ						✓	

Table 2-1. *Printer Operator and User Capabilities*

2.6 Securing the Server Console

When it comes to server security, go back to the basics: *physically isolate the server.* If the administrator's office cannot be isolated, consider placing the server is a locked closet. Next, implement full access controls to the utilities.

The MONITOR utility should be used at the server console to manage server activity and lock the console. When loading MONITOR.NLM, use the 'L' option to lock the console. This will prevent changing of server console screens until either the console password or ADMIN password is entered. Be sure to lock the console after each use. If the REMOTE utility is installed on the server and RCONSOLE is installed on the

workstation, the administrator will be able to manage the server remotely from the workstation. In this case, *be sure to use a strong password* (if there is such a thing), and *be sure to use the 'encrypted' option.*

Another word of warning: If the administrator has logged onto the server using RCONSOLE and the server should crash and reboot itself before SPX times out (2 to 3 minutes), the remote administrator will be automatically rejoined to the server when it comes back up. However, the server will *NOT* be aware of the remote administrator. Therefore, if the server should crash while the administrator is using RCONSOLE, the administrator must either shut down the workstation or stay there until the server comes back up and then logout of RCONSOLE. The use of RCONSOLE is discouraged in sensitive environments. If it is installed, be very careful with the password. If the password is compromised, the network is extremely vulnerable.

The SECURE CONSOLE utility should be used in Navy environments. It increases security by removing DOS from the server, preventing keyboard entry into the operating system debugger, preventing loadable modules (NLMs) from being loaded from any directory other than SYS:SYSTEM, and preventing the server date and time from being changed. Any attempt to exit NetWare to DOS would result in the server being locked, requiring a cold boot to restart. The only way DOS can be accessed when SECURE CONSOLE is being used is to shut down the server and bring it back up. This safeguard supports the reliable use of security and accounting features that depend on date and time for their enforcement, and prevents the loading of Trojan Horse software or virus-ridden software from DOS partitions, diskette drives, or other directories.

For more information on console security utilities, see [NOVELL 94U].

2.7 Monitoring and Auditing

The AUDITCON utility allows auditing to be accomplished independently at the volume level and the container level (Organization or Organizational Unit) by special users called Auditors, rather than the NetWare administrator. Auditing can be used globally to monitor all NDS and file system events throughout a volume, can be tailored to monitor a particular event for all users (including the administrator) or to monitor all events for a particular user or file, or some combination.

When auditing is enabled for a container, it is not automatically enabled for subordinate containers and, if desired, must be manually turned on for the volume, then set to audit the specific subdirectories as well. Any subdirectories that are added after auditing is activated will be included in the audit window. Two passwords are used for each auditor; one controls read access to the audit information, and the other controls access to all other AUDITCON capabilities (e.g., selecting events to audit, mounting a volume, creating report filters). The Auditors can, and should, *change the auditor passwords* to prevent others (including the administrator) from gaining access. Audit files are voluminous, but can be sorted and reviewed using Report Filters in AUDITCON.

Error messages that are displayed on a server console will eventually scroll off the screen and be lost. CONLOG.NLM should be installed to capture error messages for the server and store them in the \ETC directory in a file called CONSOLE.LOG. Activation of CONLOG is particularly important during system initialization and start-up. This can be done through the use of LOAD and UNLOAD commands in the AUTOEXEC.NCF file.

Audit trails have explicit size limits. It is important that the size be set high enough that the audit trail will *never* fill up. If it becomes full, auditing will cease. While it is possible to set NetWare so that the volume will be dismounted on overflow, this is not a good idea either because the audit file resides on the server in the SYS: volume where the NDS database resides (in a hidden file). Dismounting of the volume would shut down NDS. Likewise, it is recommended that user files and print queues be stored on volumes other than SYS: to avoid filling the volume and shutting down NDS.

The NetWare administrator should periodically monitor server activity. For example, to see what users are actively connected to a server and their network address, type:

NLIST USER SHOW "LOGIN TIME", "NETWORK ADDRESS" /A/S

Another way of monitoring activity on a server is to use MONITOR. The FILE OPEN/LOCK ACTIVITY option will provide a list of volumes on the server. The administrator can navigate through the list to any particular file and view the connection numbers to the file in order to determine the current users of the file. Alternately, the administrator can use the CONNECTION INFORMATION option to view a list of files any particular user currently has open.

Security audits of all file system and NDS rights should be created periodically by the NetWare administrator. The following procedure will create lists showing file system and NDS rights assignments and all mappings. The two files created by this procedure can then be viewed and manipulated with the EDIT command:

```
F:
RIGHTS /T/S > H:RIGHTS.FS
CX /R
NLIST * /D/S > H:RIGHTS.NDS
```

Where

F: is the file system Drive Map
/T indicates the option to view trustee assignments
/S indicates the option to view subdirectories
H:RIGHTS.FS is the name of the file for the file system security audit log
(of course, H: is mapped)
/R indicates to change context to the NDS [ROOT] directory
'*' indicates all classes of objects
/D indicates the option to view property details
/S indicates viewing of all levels of subdirectories is desired
H:RIGHTS.NDS is the name of the file for the NDS security audit log.

2.8 Backup and Recovery

NetWare includes the SBACKUP utility which allows the administrator to use the Storage Management Services (SMS) to backup and restore data located on various server and workstation targets and to create backup session logs and error reports. SMS consists of software NLMs (server, workstation, and database Target Service Agents; Storage Management Data Requester; Storage Device Interface; and storage device drivers) which allow backup and restore to be performed regardless of the platform and operating system (i.e., DOS, OS/2, MS Windows, Macintosh, or Unix). SBACKUP resides on the server and Target Service Agents reside on the server or workstation where the files to be backed up are located.

The frequency of performing backups is an individual decision. In general, daily backups are advised for servers. The administrator who is responsible for performing the backups must have the NDS Browse and Read rights and file system Read and File Scan rights:

NDS Object Rights	NDS Property Rights	File System Rights
[B]	[R]	[R F]

During the backup, if the session cannot fit on the media, the administrator is prompted for additional media and SBACKUP waits until the media is inserted. If additional media is not inserted, SBACKUP does not complete and does not EXIT, thus leaving SBACKUP as an active process with privileges because SBACKUP opens MONITOR, leaving the server unlocked until the second tape is mounted. If backup is scheduled for a time when the administrator is not available to attend the backup, the failure to EXIT could compromise security. Unauthorized users could perform unauthorized acts, including loading unauthorized NLMs on the server. Therefore, *always be sure the tape is large enough to support the backup, or attend the backup.*

There are three types of backups: full, incremental, and differential. A full backup is the best, but it also takes the longest. Always take full backups before and after the system is to be reconfigured or upgraded to a new version of NetWare. Try to perform the backups during "off" hours to minimize the impact on the user community. In terms of periodic backups, as a rule of thumb, if a full backup can be taken in four to five hours, take a full backup daily. Otherwise, take incremental or differential backups daily and take a full backup once per week. Differentials are better than incrementals because they backup everything that has been created or modified since the last full backup, but incrementals are faster because they only backup what has been created or modified since the last incremental (yesterday). Typically, incrementals are taken. This means that to restore the system requires restoring the last full backup and all incrementals taken since the full backup.

Entering "NO" when prompted on whether to "Append to Previous Sessions on Media" means that *append* is not desired and the new data will overwrite anything on the media. Be careful not to overwrite previous backups that should be kept (such as

overwriting a full backup with an incremental backup, or overwriting an incremental before another full backup is taken). Entering "YES" means that *append* is desired. Appending must be done to the last tape in the previous session. If you try to append to the first tape of a two-tape backup, the second tape may never be recoverable even though it has not been overwritten.

NetWare administrators are reminded that backup tapes wear out just as audio and video cassette tapes wear out at home. To help ensure that valid backups are being created, administrators should periodically – perhaps every two weeks – perform file restorations of a few files. The frequency and quantity of file restoration exercises should be based on the value and criticality of the data.

There are many third-party products that can be used by individual users to backup their own files. However, the administrator should use SBACKUP. DOS BACKUP should not be used because it will not backup all NetWare file and directory attributes.

For an excellent discussion on backup procedures, refer to [LAWREN 93]. For details from Novell's perspective, refer to [NOVELL 94R] and [NOVELL 94S].

2.9 Authentication

Authentication is a service that operates in the background to guarantee the authenticity of the sender of data or a request. NetWare 4.X authentication also checks that the traffic originated from the workstation where the authentication data was created. The user enters their password to authenticate themselves locally during logon, and NetWare generates authentication information that is transmitted over the network. The authentication mechanism is based on public key cryptography whereby the sending station digitally signs the message with their private key and the receiving station verifies the signature using the senders public key. Since no other party could have used the private key to sign the message, it is assumed that the message must be authentic. It should be noted that authentication does not protect the data in the message, only the authenticity of the message.

2.10 Service Assurance

An uninterruptible power supply (UPS) is a common piece of equipment that is used in any computing environment to provide service assurance in times of power outages. A UPS is essential for servers whenever transients are common to the public utility. A UPS should be considered even when the public utility is quite reliable if the server provides critical support for the organization. In addition, if the UPS does not include surge protection, do not buy it. If you are not sure whether the proposed UPS includes surge protection, look for information on "switchover time". Switchover time indicates surge protection may not be included because the best type of UPS always supplies power to the equipment and is constantly being recharged by the public utility, which means there would be no switchover time. If the UPS has no surge protection and is

already in your inventory, install surge protection to protect the UPS. Configure the server (SERVER.CFG) to monitor the UPS and recognize when the public utility is not providing power. The server can then send a notice to users that the system may go down soon, reminding them to save their files, and it can close open files and shut itself down after a period that you specify. Unfortunately, NetWare UPS capabilities are not able to save open files at workstations.

When designing the NetWare 4 system, it is important to incorporate redundancy of important servers, in particular the application server, to provide reliability and availability. Sooner or later, a hard disk will fail and will have to be replaced. Multiple application servers should be established for all but the smallest and least critical environments because redundancy increases reliability. In larger environments where downtime cannot be tolerated, redundancy should be installed for other critical servers as well. Disk duplexing, shown in **Figure 2-12**, should be implemented in any environment where the organization cannot accept downtime of 24 hours or more. Explain the importance of disk redundancy to management and use all your persuasive powers to convince them to implement disk duplexing, or at least disk mirroring. *If management is opposed to disk duplexing, request a written waiver that states fault tolerance is not an issue.*

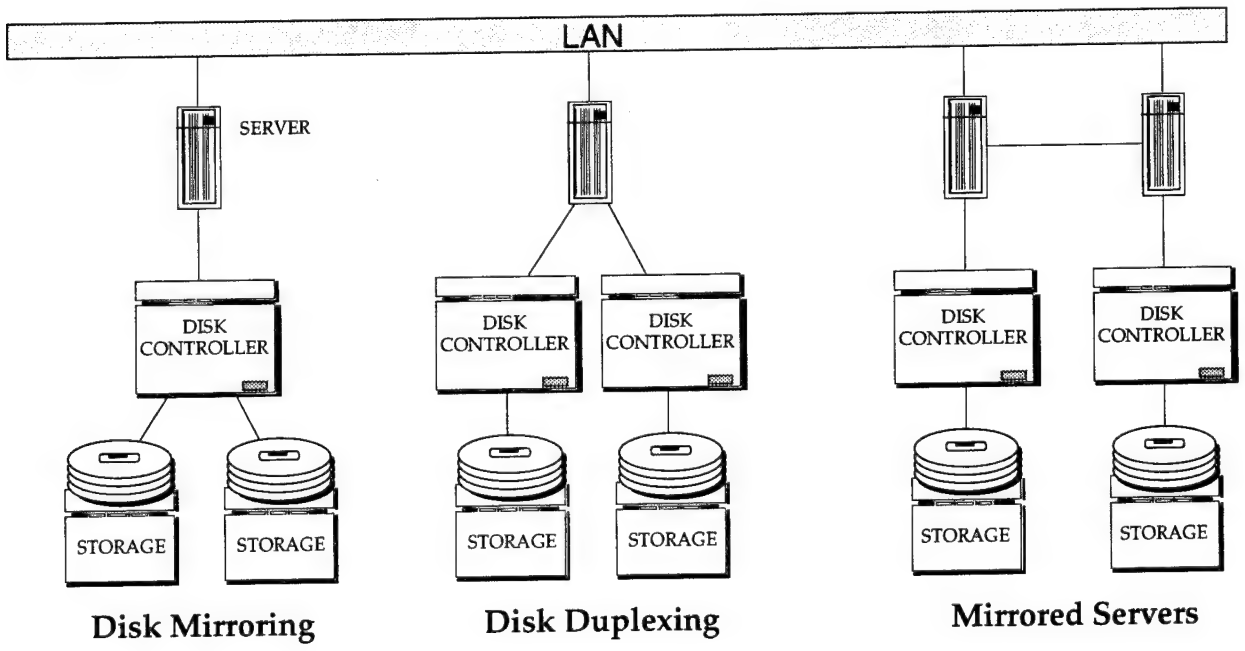


Figure 2-12. *Redundancy Techniques Provide Fault Tolerance*

Another critical issue on disk redundancy concerns how volumes will be assigned. A volume can reside on a single hard drive or can "span" multiple hard drives. The advantage of spanning is that it increases speed, particularly if the server is a database server and records can be written to several hard drives at once. The disadvantage is that there are more drives that could fail and if any one of the drives fails, the entire volume is inaccessible. Therefore, *if spanning is desired for performance, disk mirroring must be implemented so there is always a hot backup for each hard disk.* Mirrored servers can be installed for extremely critical applications. Disk mirroring, disk duplexing, and mirrored servers are relatively expensive because they involve significant amounts of additional hardware. The payoff is fault tolerance and improved performance. One other note: a list of Novell certified hardware can be obtained by calling 1-800-NETWARE.

NetWare 4 includes the Transaction Tracking System (TTS) to protect data from corruption by backing out and logging incomplete transactions that occur when a component of the network fails (server or workstation hardware or software, or communications hub, repeater, or cable). The transaction that failed is backed out immediately if the failure occurs in a workstation or the network, or after the server is brought back up if that is where the failure occurs. TTS supports both applications with and without built-in transaction backout capabilities. *Do not disable TTS on a server.* This would prevent the NDS Directory tree from being updated on that server.

For more information on disaster recovery and disk redundancy, see [SHELDON 94] and [LAWREN 93].

This Page Intentionally Left Blank

Section 3

Third Party Security Products

This Page Intentionally Left Blank

3.0 Third-Party Security Products

Existing security features of NetWare do not provide all of the protection that is needed for some sensitive environments. Other areas of interest include access controls for the workstation, enhanced authentication that incorporates one-time passwords, data encryption, network analysis and management, audit reduction, firewall security, and virus protection. Vendors have develop hardware and software products for each of these security areas. While most of the products discussed in this section operate independent of NetWare, they all function well in a NetWare environment. Some are designed as Virtual Loadable Modules (VLMs) which are executable files (EXE) installed on the workstation that load the DOS Requester software. The DOS Requester determines whether service requests should be directed to DOS on the local workstation or to NetWare on the server. A few are designed as NetWare Loadable Modules (NLMs) which are installed on servers to expand the functionality of the NetWare operating system. These are tightly coupled with the operating system and have instant access to other operating system services.

3.1 Workstation Access Controls

There is a large selection of access control products, second only to those for virus protection. Access controls are important since NetWare cannot prevent unauthorized users from gaining control of the workstation or the files on the workstation. Features to look for are implementation in hardware, boot protection, and prevention of access to DOS. Other desirable features include data encryption, virus protection, and memory clearing to purge memory of residue upon deallocation.

Three vendors – Mergent International, Cordant, Inc., and Fischer International – are particularly well known for their workstation access control products. The products of these three plus two relative newcomers with products that operate in a NetWare environment are shown in **Table 3.1** along with a description of their features. Mergent's focus is to provide enterprise-wide security products for PCs and NetWare servers. PC/DACS is NCSC-certified. Cordant was selected by Novell to participate in their trusted network computing initiative to help develop NetWare products that can be submitted for TCSEC C2 and ITSEC E2 evaluation. Fischer was one of the first vendors of mainframe and PC access controls. PC Guardian and Trend Micro Devices do not have the credentials of the major three, but have received very positive comments in commercial reviews. Other well known vendors of access control products include:

- Uti-Maco Safeguard Systems, 250 Old Main, Rocky Hill CT 06067, (800) 394-4230 – Products: SafeGuard Professional for DOS & Windows, LAN-Crypt, CryptMail for DOS & Windows, SmartCards

- PC Security Ltd., Window House, Spittal St., Marlow, SL73HJ, U.K.
  Products: Stoplock V (access control, data encryption, full network security management), AccessManager (authentication), LapGuard (for portables)

Table 3-1. *Access Control Products*

Product	Vendor	Features	Related Products
PC/DACS for DOS & Windows (known as PC-Guard in Europe)	Mergent International 70 Inwood Rd. Rocky Hill, CT 06067 (800) 688-3227	- Hardware boot protection - Identification and authentication - Session time-out - Encryption (DES) - Virus detection	- Net/DACS (for Novell server) - SSO/DACS (single sign-on) - Domain/DACS (for central monitoring and management)
Assure	Cordant, Inc. 11400 Commerce Park Dr. Reston, VA 20091-1506 (800) 843-1132	Hardware/software for NetWare workstations under DOS or Windows - Boot protection - Single sign-on - Digital signature - Encryption (DES) - Smart card tokens	- Assure Server NLM (for client to server security) - Assure ASCA (smart card access API) - Assure/Com (encrypts dial-in communications) - Assure Tiro (secure telecommunications)
Watchdog Armor	Fischer International 4073 Mercantile Avenue Naples, FL 33942 (800) 237-4510	Hardware/software for NetWare workstations - Boot protection - Encryption (DES) - Secure clock - Memory clearing - Virus protection - Audit trail	- Watchdog Director (to manage all Watchdog profiles in the network) - Mail Safe (signature) - Watchdog PC Data Security - SecurID Card (60 sec. passcode smart card)
Network Security Plus (for NetWare)	PC Guardian 1133 Francisco Blvd. East Suite D San Rafael, CA 94901-5427 (800) 288-8126	Works with NetWare SYSCON utility to directly connect user to NetWare during boot - Single signon - Central management - Access control	- Encryption Plus - Floppy Drive Locks (physical devices) - Keyboard Locks (physical devices) - Anti-theft cabling
StationLock for NetWare (client for workstation and NLM for server)	Trend Micro Devices, Inc. 2421 W. 205th Street Suite D-100 Torrance, CA 90501 (800) 228-5651	Hardware product; Proprietary BIOS in ROM; takes control of the workstation prior to loading operating system - Access control - Virus protection	- Chip Away Virus - PC Rx LANPack - T-Lock for DOS and Windows - PC-cillin LANPack

- Computer Associates International, Islandia, NY 11788, (800) 225-5224
  Products: CA-Unicenter, CA-Cortana, CA-Top Secret/PC, CA-ACF2/PC
- Cassidy and Greene, Inc., 22734 Portola Dr., Salinas, CA 93908, (800) 359-4920
  Products: Access Management Environment (for Macintosh).

3.2 Authentication

NetWare's authentication capabilities include mechanisms that require users to identify themselves with a userid and password, and for workstations to protect that authentication information during transmission to the server and to include workstation identification information as well. This type of user authentication is based upon *something the user knows.* For most organizations operating NetWare networks within their facilities, this provides an acceptable level of security. However, it is possible for the authentication information to be intercepted and for an imposter to masquerade as a valid user, especially if the network exits the facilities into nonsecure areas.

When the sensitivity of the data merits additional security, or when the network is not wholly confined within the facilities, stronger authentication may be appropriate. Other mechanisms strengthen the authentication capability by implementing "two factor" authentication, i.e., by requiring users to submit further evidence of *who they are* or to present *something they possess.* Authentication based on user characteristics generally involve biometric devices that read a retina print, fingerprint, palm print, voice print, or saliva print (just kidding). Biometric devices are relatively expensive and are more commonly associated with access to a computer facility than to user workstations.

Smart card technology has progressed so that authentication based upon something the user possesses can be added to the workstation. There are two standard sizes of smart cards: one is a little thicker than a typical credit card and displays information in an LCD window; the other is a little smaller than a diskette and conform to the standards of the Personal Computer Memory Card International Association (PCMCIA). The smaller card is not inserted into the workstation, but provides information to the user. The PCMCIA card is inserted into an expansion memory slot on the computer or a peripheral card reader connected to the parallel port and interfaces directly with the system. Most card readers are compatible with existing LAN card standards, so drivers that are included with NetWare can be used. [SHELDON 94]

Smart cards incorporate microprocessors and are capable of supporting time-based passwords which change every 60 seconds or one-time passwords (i.e., implements a challenge-response sequence to generate a new password for each logon). The advantage of one-time and time-based passwords is that if they are intercepted on the network, they cannot be reused in the future. Smart card technology will become even more important as users become more mobile, logging on from workstations anywhere in the network, or even from outside their local area.

Security Dynamics, listed in **Table 3-2**, produces the SecurID Card which calculates a time-based PASSCODE and displays that code for the user to see and enter manually into the workstation. SecurID operates in conjunction with the ACE/Client for NetWare NLM and ACE/Server products. PASSCODEs are recalculated every 60 seconds. The ACE/Server can be implemented as an Application Program Interface (API) that is callable by application programs. The advantage of this is that applications can request reauthentication periodically to verify that the authorized user is still present. The user

Table 3-2. *Authentication Products*

Product	Vendor	Features	Related Products
SecurID Card	Security Dynamics One Alewife Center Cambridge, MA 02140 (800) SECURID	- Convenient (software only; no card reader) - Time-based - Credit card size - Audit trail	- ACE/Client for NetWare NLM - ACE/Server - ACE/Client for NT/RAS (Windows NT)
SecureNet Key	Digital Pathways, Inc. 201 Ravendale Drive Mountain View, CA 94043 (800) 344-7284	- PCMCIA Card - Challenge-response - DES - Reprogrammable card - Audit trail - Works with Sidewinder Firewall	- Defender Security Server NLM - Software SecureNet Key
CyberSAFE Challenger	CyberSAFE Corp. 2443 152nd Avenue, NE Redmond, WA 98052 (206) 883-8721	- Kerberos - DES - Mutual authentication - Integrity - Nonrepudiation - Data confidentiality - Audit trail - Works with SecurID	- CyberSAFE Application Security Toolkit (GSS-API compliant)
SSO/DACS	Mergent International 70 Inwood Rd. Rocky Hill, CT 06067 (800) 688-3227	- Single sign-on - NetWare environments	- Net/DACS
Access Manager	ICL Enterprises 11490 Commerce Park Dr. Reston, VA 22091 (703) 648-3300	- Dedicated Unix server - Works with badge readers and smart card systems	–

then looks at and enters the SecurID PASSCODE calculated for that moment. The ACE/Server provides centralized authentication, administration, and auditing but requires a dedicated server. The ACE/Client NLM transmits the credentials to the ACE/Server for authentication before the user is logged into NetWare. The process is transparent to the user. SecurID and ACE/Client for Novell NLM work on workstations attached to the network. They also work in conjunction with Novell's NetWare Connect which provides security for dial-up ports. The disadvantage of SecurID is that when the cards expire (from one to four years) they must be discarded and new ones purchased.

Digital Pathways produces the SecureNet Key which is a PCMCIA product that operates in conjunction with their Defender Security Server NLM to implement

challenge-response authentication using one-time passwords. DES is used to protect the challenge-response exchange. The SecureNet Key card can be reprogrammed when a user suspects their Personal Identification Number (PIN) has been compromised or when the battery is changed in the card. Defender Security Server provides centralized authentication, administration, and auditing but requires a dedicated server, and is not as compatible with NetWare as is the ACE/Server which supports the SecurID Card. SecureNet Key is best suited for remote workstations that must dial into the NetWare network. In this case, the Defender Security Server interfaces between the modem pool and the NetWare server to provide authentication. SecureNet Key also works with Secure Computing Corporation's Sidewinder Firewall for authentication of users accessing the NetWare network from external networks. The non-PCMCIA implementation of SecureNet Key is called Software SecureNet Key. This eliminates the requirement for a PCMCIA card reader, but increases the risk to the algorithm, though it is encrypted and can be required to be installed from diskette during each use. There are versions for DOS, Windows, and Macintosh environments.

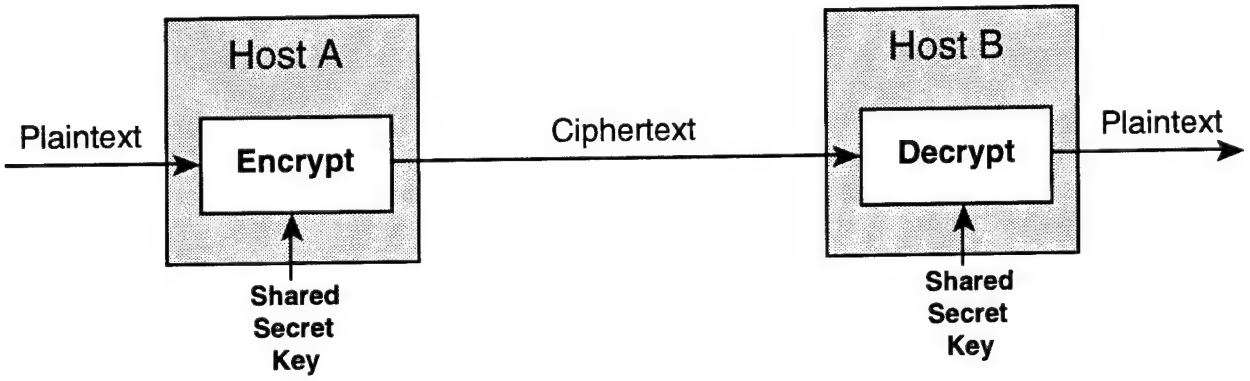
CyberSAFE Corporation produces CyberSAFE Challenger. CyberSAFE Challenger implements Kerberos, a software-based authentication mechanism developed by MIT. The Kerberos architecture uses a trusted third party (the Kerberos Authentication Server) to interfaces with the client and the server in secure (DES) exchanges. The use of DES provides confidentiality and authentication services. These services can be extended to the message traffic. Kerberos also uses a checksum to provide integrity. In addition, the Kerberos Authentication Server supports nonrepudiation for both sender and receiver. Kerberos also implements mutual authentication. This is important because hosts that do not authenticate themselves to the user can be spoofed by an adversary who can pose as that host to intercept authentication information from the user, then pose as the user in accessing the host. CyberSAFE is supported in NetWare environments and on DOS, Windows, Macintosh, and other platforms. Furthermore, it can be implemented in conjunction with Security Dynamic's SecurID Card.

Another authentication capability called "single sign-on" offers advantages and disadvantages. With single sign-on, once the user has signed onto the network, the authentication mechanism automatically logs them onto other applications or servers for which they are authorized access. In particular, users of database applications find single sign-on to be more expedient. From a security perspective, an advantage is that users have only one password to remember and are less likely to write it down than when they have several to remember. The disadvantage is that if the password is compromised, the adversary has access to all systems for which the user is authorized access. Oracle Corporation, Software AG, and other vendors working with database management systems are developing single sign-on applications.

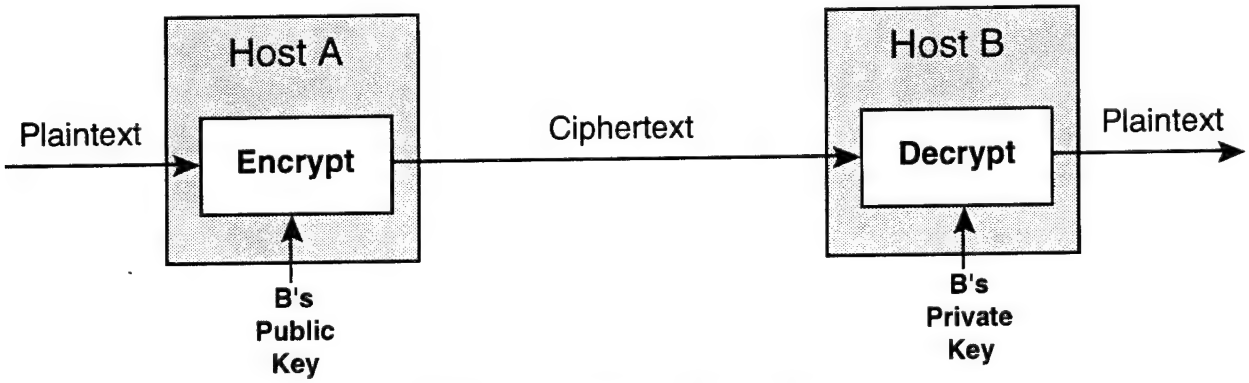
Mergent International, discussed in **Section 3.1** under Workstation Access Controls, produces Single Sign On (SSO/DACS) which operates in conjunction with their access control products at the workstation level. SSO/DACS includes predefined templates for Novell NetWare as well as for other network operating systems. ICL Enterprises produces Access Manager, a single sign-on product that is also compatible with other access control products including badge readers and smart card systems.

3.3 Encryption

Encryption, the science of scrambling and descrambling data streams so the information is meaningless to anyone who intercepts it, is complex and is beyond the scope of this handbook. Briefly, there are two basic types of encryption: symmetric and asymmetric. Symmetric encipherment, also referred to as *pairwise, secret key, one-key,* or *conventional encipherment,* transforms plaintext into ciphertext through the use of an encryption algorithm and a secret key that is shared by two parties, as shown in **Figure 3-1(a)**. Asymmetric encipherment, also referred to as *public key* or *two-key encipherment,* involves an encryption process that uses one key, called a public key, and a decryption process that uses another key, called a private key. The sender encrypts a message with the *receivers public key* and the receiver decrypts the message using the *receiver's private key.* Public keys cannot be used to infer private keys and therefore require no protection from compromise and can be widely distributed. Private keys are not shared and must be protected from compromise.



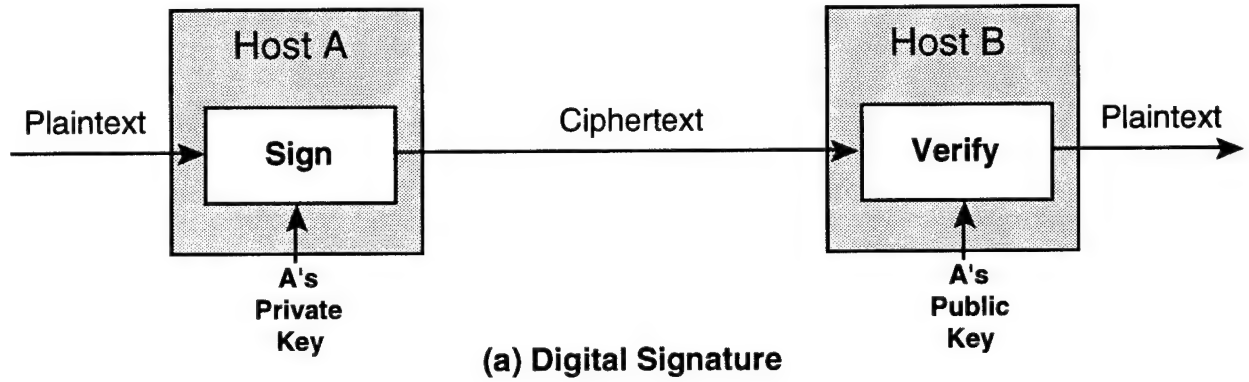
(a) Symmetric Encryption



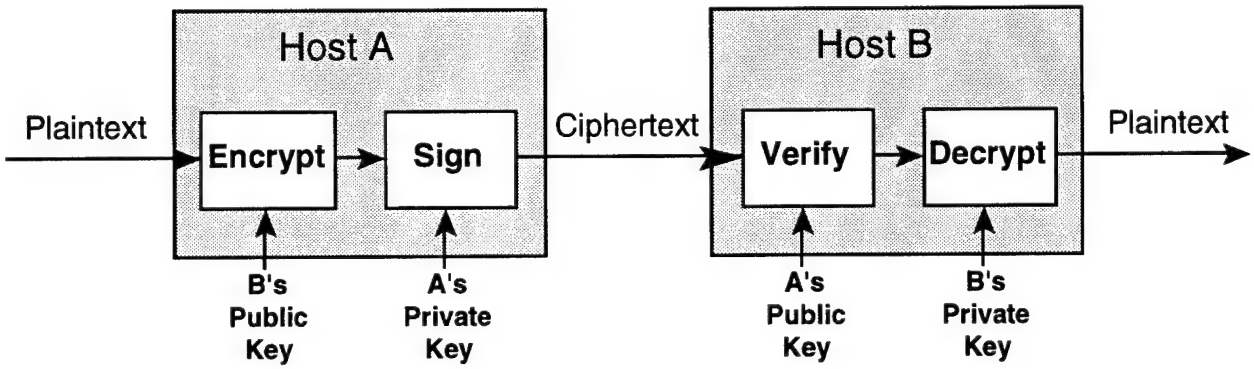
(b) Asymmetric Encryption

Figure 3-1. *Conventional and Public Key Encryption Methods*

Conventional encipherment, used in most classified military communication systems, is appropriate for protection of point-to-point communication channels. It offers faster throughput than public key encipherment but requires that each pair of hosts share a unique key. Pairwise keying provides authentication of communications between two hosts since no other party shares that key. Public key cryptography, on the other hand, allows for wide distribution of encryption keys since possession of the public key only allows the holder to encrypt traffic but not decrypt the traffic. A limitation of public key encryption is that it does not authenticate the sender since anyone could have used the public key to encrypt the traffic. To add authentication, the sender would also have to encrypt the traffic with their private key (digital signature); the receiver would use the sender's public key to decrypt the message (verify the signature), as shown in **Figure 3-2**. In addition, integrity is not supported because asymmetric encipherment does not provide error extension. Public key encipherment is processing intensive and is not suitable for providing data confidentiality. The best use of public key encipherment is to distribute secret keys for conventional encipherment, and then to use conventional encipherment for data confidentiality.



(a) Digital Signature



(b) Confidentiality and Authentication

Figure 3-2. *Public Key Encryption for Digital Signature*

There are various algorithms that are used for conventional encryption. Those that are authorized for classified processing are controlled by the National Security Agency (NSA) and keys are distributed by NSA. The Data Encryption Algorithm (DEA) is not authorized for use in classified environments, but is authorized for sensitive unclassified environments and in the commercial arena, and key distribution is managed by individual organizations. Though DES is authorized for commercial use, export restrictions do apply. The DES is considered to be relatively weak and may be breakable in the future as faster computers are developed. Accordingly, the government has sought a replacement algorithm. The banking industry and others have not been receptive to this idea because of their significant investment in DES hardware.

A new encryption method, called *Escrowed Encryption* [NIST 94E] has been developed for commercial environments, both domestic and international. Escrowed encryption implements the SKIPJACK algorithm which includes a Law Enforcement Access Field (LEAF) that provides a "back door" key that can be used to "wiretap" encrypted traffic. The "back door" escrow key is broken into two parts, each held by separate escrow agents. Currently, the escrow agents are government agencies (National Institute of Standards and Technology and the Department of the Treasury), but a public cry of "Big Brother is watching" has caused the government to consider placing one of the escrow half-keys in the control of a private corporation. Foreign governments have also indicated a desire to hold one of the half-keys in communications that involve their nations. If the escrow agents were to join forces to eavesdrop on someone, they would not be able to do so without first obtaining the Family Key which is used to identify the Serial Number of the encryption device. This is needed in order to determine which Escrow Key to use. The Family Key is held by a third government agency (Federal Bureau of Investigation), and policy prevents its release without a court order (Department of Justice). Thus, four agencies must collaborate in order for eavesdropping to occur.

Other encryption algorithms that are considered to be much stronger than DES have also been developed. The best known in Pretty Good Privacy (PGP), which is a public-domain program developed by Phil Zimmermann and placed on the Internet for wide dissemination. PGP implements the International Data Encryption Algorithm (IDEA), a symmetric algorithm considered to be much stronger than DES. It provides data confidentiality for electronic mail and is used in file encryption applications. The government is opposed to it's use since it does not include a LEAF and may be used for criminal activity with relative assurance of privacy.

Encryption is one of the most important security services that can be implemented in environments where privacy is an issue. Some algorithms also provide integrity assurance because a corrupted message cannot be decrypted into meaningful plaintext. Products that use DES for data confidentiality include PC/DACS for DOS & Windows, Assure, and Watchdog Armor (all discussed in **Section 3.1**, Workstation Access Controls), listed in **Table 3-3**. Another impressive line of encryption products are the Network Security System (NSS) developed by Semaphore Communications Corporation. The NSS consists of the Network Security Center (NSC) and a variety of

Table 3-3. *Encryption Products*

Product	Vendor	Features	Related Products
PC/DACS for DOS & Windows	Mergent International 70 Inwood Rd. Rocky Hill, CT 06067 (800) 688-3227	- Encryption (DES)	- Net/DACS (for server) - SSO/DACS (single sign-on) - Domain/DACS
Assure	Cordant, Inc. 11400 Commerce Park Dr. Reston, VA 20091-1506 (800) 843-1132	Hardware/software for NetWare workstations under DOS or Windows - Encryption (DES) - Smart card tokens	- Assure Server NLM - Assure ASCA - Assure/Com
Watchdog Armor	Fischer International 4073 Mercantile Avenue Naples, FL 33942 (800) 237-4510	Hardware/software for NetWare workstations - Encryption (DES)	- Mail Safe - Watchdog PC Data Security - SecurID Card
Network Security System (NSS) – Network Security Center (NSC) – Network Encryption Units (NEUs)	Semaphore Communications Corp. 2040 Martin Avenue Santa Clara, CA 95050 (408) 980-7750	- Certificates (RSA) Encryption (DES) - Central management, audit, key distribution - Integrity (ICV) - Authentication - Access Control	- NEU-ST (site-to-site) - NEU-PC (workstation) - NEU-WG(work group) - NEU-EN (department)
Encryption Plus	PC Guardian 1133 Francisco Blvd. East Suite D San Rafael, CA 94901-5427 (800) 288-8126	Encryption of data as it is stored to or retrieved from hard disk - Has master password to prevent lockout - Can import/export encrypted files	- Network Security Plus
Fortezza Crypto Card – Clipper Chip – Capstone Chip	Mykotronx, Inc. 357 Van Ness Way Suite 200 Torrance, CA 90501 (310) 533-8100	Implements SKIPJACK algorithm with LEAF - Confidentiality - Integrity - Authentication - Nonrepudiation	–
Secret Agent	AT&T Secure Communications Systems P.O. Box 20446 Greensboro, NC 27420 (800) 243-7883 Developed & marketed by: Information Security Corp. 1141 Lake Cook Rd, Ste D Deerfield, IL 60015 (708) 405-0500	- Key exchange (RSA) - Encryption (DES) - Exportable algorithm - Supports access control boards - Supports crypto cards	- Secure ZMODEM - SpyProof - DSA Signature Software - (future) Interactive Terminal Session Encryption

Network Encryption Units (NEUs) which are RISC-based processors that process data at speeds of up to 100 Mbps and are about half the size of a notebook computer. The NSS uses RSA public key encryption for electronic key distribution of DES keys, which are in turn used for traffic encryption. NEUs can be installed on workstations, servers, printers, and mainframes on a NetWare network or virtually any other network operating system or protocol, including Ethernet and Token Ring. NEUs can also be used to link sites via either frame relay or switched multi-megabit data service (SMDS). The NSC provides central management, key certification, and central auditing. In addition to confidentiality, the NSS provides cryptographic integrity based on an integrity check value (ICV), source host authentication, and access control during transmission.

Encryption Plus is a product developed by PC Guardian to work with Network Security Plus (discussed in **Section 3.1**) in a NetWare environment to provide data encryption of information as it is stored from RAM to disk and decryption upon retrieval. It encrypts data streams rather than files. The primary purpose is to prevent the storage of unencrypted information on the hard disk. Encryption is transparent after logon when the password is entered, and it encrypts at a speed of approximately 10 megabytes per minute. The product can be used to encrypt files for transmission, though it is not as convenient as the three DES products discussed above. To encrypt files for transmission, the encrypted file is *imported* into RAM and then transmitted over the network. Since the encryption key is generated from the password, called the *privacy code*, the receiving host must have the same password in order to decrypt the file. The software is installed on workstations remotely from the NetWare server by the NetWare administrator and has a Master Password that permits administrator access through a back door; it's purpose is to ensure access if a Privacy Code is lost or an employee leaves the company. Encryption Plus uses a proprietary algorithm developed by Compaq, which is not considered as secure as using DES. The algorithm is exportable.

Mykotronx, Inc. developed the first key escrowed systems, called the *Fortezza Crypto Card,* which incorporates the Clipper and Capstone chips that implement the SKIPJACK algorithm. Clipper provides confidentiality only; Capstone provides confidentiality, key certification and exchange, digital signatures (Digital Signature Standard, DSS and Secure Hash Standard, SHS) for authentication, nonrepudiation, and data integrity. Fortezza Cards are PCMCIA compliant and work with access control boards. They do not typically have a user interface and require another product for that.

AT&T markets a software product called *Secret Agent* (originally developed by Information Security Corporation and still marketed by ISC for AT&T) that enhances the capabilities of the access control boards (e.g., Fischer Armor, Cordant Assure) and the PCMCIA smart cards (e.g., Mykotronx Fortezza Card, Datakey Inc. SignaSure Card) for DOS, Windows, Macintosh, and other platforms. With regard to the access control boards, Secret Agent adds public key (RSA) encryption for key exchange and digital signature (DSS) for authentication. With regard to crypto cards, Secret Agent provides the user interface. In addition, Secret Agent can perform bulk encryption using DES, Triple DES, Skipjack (using Mykotronx Fortezza Card), International Data Encryption Algorithm (future), or an exportable proprietary algorithm. Organizations can install Secret Agent by itself to perform authentication, key exchange, and bulk encryption

services, or they can augment it with Fortezza (since encryption performed in hardware is stronger than in software) and have the Fortezza card be supported by the Secret Agent user interface. Secret Agent does not encrypt transmission streams; it encrypts files that are selected by the user. It works well in a NetWare environment. A future enhancement to this family of products will be an interactive terminal session product.

Two other encryption products with a strong reputation in NetWare environments, but not specifically designed to run under NetWare nor developed by vendors of access control products, are the following:

- Variable Encryption Intelligent Labeling (V.E.I.L.) is a key management system for Windows environments – Vendor: Eldyne, Inc., Four Crystal Park, Suite 709, 2345 Crystal Drive, Arlington, VA 22202, (703) 414-8944

- Toolkit for Interoperable Privacy Enhanced Messaging (TIPEM) allows programmers to develop secure interoperable messaging, mail, workflow, and forms applications using symmetric (DES and proprietary) and asymmetric algorithms for confidentiality and digital signatures – Vendor: RSA Data Security, Inc., 100 Marina Parkway, Suite 500, Redwood City, CA 94065, (415) 595-8782.

3.4 Network Analysis and Management

This section discusses products that provide network analysis and management. As networks grow, performance drops. It is important that the administrator check for improperly configured network components and overworked servers. Protocol analyzers (i.e., sniffers) determine which workstations are the most active and which are generating errors, capture and view specified packets, establish short-term and long-term trends concerning network performance, send alerts to the administrator, and load test the network. These tasks help determine when an administrator should install another LAN segment, replace a network adapter, adjust the broadcast frequency of servers and routers to reduce traffic, determine the type of traffic on the LAN, predict future loads, react to surges and errors, and check transmission delays, adapters, and cabling. This section does not include analysis tools designed for wide area networks (WANs), which are useful in evaluating the effectiveness of firewalls (they are discussed in **Section 3.5**), or virus protection products (they are discussed in **Section 3.6**).

Novell offers a suite of management tools for NetWare, called ManageWise, which consists of the NetWare Management System (NMS), NetWare LANalyzer Agent NLM, LANDesk Manager, LANDesk Virus Protect (from Intel Corporation), and Net Explorer. ManageWise, listed in **Table 3-4**, detects server problems, including break-in attempts, and network problems, such as network interface cards that are about to fail. It performs network analysis (e.g., congestion, error packets) and traffic analysis (e.g., identifies nodes with the heaviest traffic, duplicate IP addresses), takes hardware and software inventories, sends alerts to the administrator's console, and works with third-party management (SNMP) consoles (there are more than 85 hub, router, and console "snap-in" products for ManageWise). ManageWise does not provide all the

Table 3-4. *Network Analysis and Management Products (Page 1 of 2)*

Product	Vendor	Features	Related Products
ManageWise: - LANalyzer Agent - Management Agent - LANDesk Manager - Virus Protect (Intel) - Net Explorer	Novell 122 E. 1700 South Provo, Utah 84606 (800) 453-1267 (800) 274-4374 LANalyzer Dept: (800) 243-8526	- Detects: server problems network problems - Network analysis - Traffic analysis - Inventory - Alerts administrator	- LANalyzer for Windows - LAN WorkPlace for DOS and Windows
Track NLM	On Technology Corp. One Cambridge Center Cambridge, MA 02142 (800) 767-6683	- High user acceptance - Detects server and network problems - Network analysis - Traffic analysis - Alerts administrator	- SofTrack (license metering)
IntroPack - NetWare Management - NetWare Early Warning System - LAN Directory	Frye Computer Systems 19 Temple Place Boston, MA 02111 (800) 234-3793	- Workstation management - File server management - Graphical displays - Enhanced security - LAN diagnostics - Report generation - Alerts administrator - Editor's choice by many magazines in 1994	- Node Tracker - Statistics Display Rack for NetWare - Alert Interface Manager - Software Metering and Resource Tracking - Software Update and Distribution System - NetWare Console Commander
Kane Security Analyst	Intrusion Detection 217 E. 86th St., Suite 213 New York, NY 10028 (212) 348-8900	Resides on PC, checks entire NetWare network - Effective rights - Password cracker - Checks resistance to packet masquerade	ShadoWare (fall '95)
BindView NCS	LAN Support Group, Inc. 2425 Fountainview, #390 Houston, TX 77057 (800) 749-8439	- Server auditing - Workstation auditing - Hardware and software inventory	- BindView Workstation Manager for NMS - Traveling BindView - NetSqueeze (compress) NLM +encryption NLM
LANDesk Traffic Analyst	Intel Corporation 734 E. Utah Valley Suite 300 American Fork, UT 84003 (800) 538-3373	- Packet sniffer - Monitors workstation utilization and errors - Reports by station and packet size - Enterprise capable	- LANDesk Management Suite - LANDesk Virus Protect

Table 3-4. *Network Analysis and Management Products (Page 2 of 2)*

Product	Vendor	Features	Related Products
Expert Sniffer Network Analyzer (for NetWare)	NetWork General 4200 Bohannon Dr. Menlo Park, CA 94025 (800) SNIFFER	- NetWare protocol suite - Portable for short-term analysis of segments - Packet sniffer	- Distributed Sniffer System - Oracle7 Database Module
LANdecoder	Triticom P.O. Box 444180 Eden Prairie, MN 55344 (612) 937-0772	- Packet sniffer - Monitors workstation utilization - Reports by station and packet size - Alarms sent to pager	- EtherVision (monitoring and reporting) - Token Vision - ArcVision
NetTools - Application Manager - IniTool .INI File Mgr - Print Manager - Desktop Control Language - Secure Station Tools	McAfee, Inc. 2710 Walsh Avenue Santa Clara, CA 95051 (800) 866-6585	- Windows management - For NetWare networks - Tied to NDS - Central management of all workstations - Restricts access to applications - Administrator override password	- NetShield NLM - ViruScan
SmartPass NLM	E.G. Software 319 SW Washington, #706 Portland, OR 97201 (503) 294-7025	- Password cracking - Database of 150,000 weak passwords	–
NetSentry	Net Inc. 20218 Bridgedale Lane Humble, TX 77338 (713) 446-2154	- Auto logoff inactive workstations - Doesn't logoff key users, groups, or applications	NETMenu

management capability needed by some administrators because it does not perform security assessment of the environment (e.g., evaluating effectiveness of intruder detection, assessing effective rights) and does not offer enhanced audit trail reduction capabilities over what is delivered with NetWare.

The LANalyzer Agent is an NLM that could be installed on any server or PC without the rest of ManageWise. Novell also produces *LANalyzer for Windows,* a standalone network analyzer which runs on a Windows-based PC for portable network analysis and troubleshooting within an Ethernet or Token Ring network segment. It can capture and analyze IPX packets, determent bandwidth usage and when peaks occur, identify stations which generate the most traffic, and identify error packets.

AuditTrack NLM (formerly known as EyeSpy) by On Technology is a NetWare tool that monitors and documents selected or all login, file, remote access, and NDS activity on NetWare servers. AuditTrack logs events to the audit trail and alerts the administrator when specific activities (i.e., unauthorized access attempts) occur. AuditTrack is installed only on the server, not on the workstation, and is transparent to the user. On Technology also markets SofTrack NLM, a well received license metering tool that helps keep the organization legal. These products are available free for 60 day trial evaluation periods. Administrators should consider these ahead of others.

Frye Computing Systems, Inc. specializes in network management utilities for NetWare. The IntroPack consists of three products: NetWare Management which consolidates information from SYSCON, PCONSOLE, FCONSOLE, PRINTDEF, PRINTCON, and FILER for diagnosis and troubleshooting purposes and maintain historical records on server activity; NetWare Early Warning System which monitors servers and workstations and sends alerts when network errors are detected; and LAN Directory which maintains hardware and software inventories. Frye's Statistical Display Rack for NetWare graphically reports the statistics in easy to read displays that look like dashboard gauges and bar charts. It can be linked to Frye utilities or to Novell's NMS and can run in the background while other Windows applications are running. Frye has a sniffer utility (Node Tracker), Software Metering and Resource Tracking utility, Alert Interface Manager for Novell NMS, NetWare Console Commander (to schedule NetWare console commands such as sending messages, loading NLMs, setting parameters, running programs, and clearing connections to take place automatically), and Software Update and Distribution System (for PCs, for Macintoshes, for WANs, and for NetWare servers). Frye products have been selected as the Editor's Choice by PC Magazine, Network Computing, InfoWorld, NetWare Connection, LAN Magazine, LAN Times, Byte, PC User, and NTSL-Software Digest in 1994 and by many in previous years.

The Kane Security Analyst (KSA) is an excellent NetWare security assessment product, developed by Intrusion Detection, Inc., that is very user friendly, requiring virtually no learning time. It evaluates user passwords and privileges on all servers on the network and produces a report card for the administrator. The strength of each password is evaluated against several rules (e.g., same as userid, reverse of userid, forced changing, length, grace logins) and a 20,000 password cracking database. The KSA also investigates and reports effective rights of user and group IDs and specifies any Userids with excessive administrative privileges. It also searches for back doors to supervisory access. It assesses the resistance of IPX packets from being forged so that a user could masquerade as the supervisor. It also reviews Intruder Detection, verifying that it is activated and whether lockout occurs properly. The KSA is a passive software product (an application, not an NLM) that runs on a Windows-based PC connected to a NetWare 3.X or 4.X (or Windows NT) network and requires administrator security equivalence privilege to function. The KSA was rated "best product of the year" for 1995 by Infosecurity News magazine. Intrusion Detection is also developing a companion product for release this year, called ShadoWare, which develops a "fingerprint" of normal activity for each userid and alerts the administrator when the user deviates from that profile.

BindView NCS by the LAN Support Group, Inc. is a more robust enterprise-wide NetWare administration tool than the KSA, but lacks some of the security administration features. The two complement each other and can be installed on the same network. BindView takes full hardware and software inventories for the network, provides information about the NLMs currently running on each file server, audits the security of the file server, performs workstation auditing, views efficiency of hard disk usage by workstation and forecasts hard disk purchase needs, and locates unauthorized programs or games on workstation hard disks.

A software-based protocol analyzer that works well in NetWare and many other networks is Intel's LANDesk Traffic Analyst. LANDesk Traffic Analyst runs on a workstation to capture packets in a Windows/DOS environment. It decodes packets, monitors any protocol conversation, creates station logs, analyzes LAN segments or the entire enterprise LAN, creates reports that include utilization, error rates, and packets per second, and can provide immediate alerts to the administrator (if installed with Novell's LANDesk Manager). Intel also makes LANDesk Virus Protect.

The Expert Sniffer Network Analyzer was developed by NetWork General specifically for NetWare networks. There are two versions, a portable (lugable with a 16-bit card) and a notebook (with a PCMCIA card). The Expert Sniffer is designed to be carried to the segment for short-term analysis. A companion product, the Distributed Sniffer System, is console-based with permanent sniffers installed on the segments for enterprise-wide network management. NetWork General offers more than a dozen two- to four-day courses on network analysis and troubleshooting. Course information is available by calling (800) 395-3151 or sending e-mail to snifferu@ngc.com.

Another software-based protocol analyzer for smaller networks is the LANdecoder for Ethernet, Token Ring, and Arcnet segments developed by Triticom. LANdecoder monitors network utilization and reports results by station and packet size. It captures packets going to or from stations specified by the administrator, can peek into packets and capture those with specified contents, or can capture packets that meet other criteria. A nice feature of LANdecoder is that it can route alarms to the administrator's pager. LANdecoder was named one of the "Top 30 LAN Products of the Year" for 1995 by LAN Magazine. A drawback is that LANdecoder is DOS-based rather than Windows-based. LANdecoder's companion product is Vision (EtherVision, TokenVision, and ArcVision), which monitors segments and produces reports.

Since NetWare runs in a Windows environment, tools for managing Windows on workstations and servers may be very helpful for NetWare Administrators. McAfee, Inc. markets NetTools for centrally managing Windows and configuring applications in NetWare networks (there are also Microsoft NT and Banyan Vines versions). NetTools allows the administrator to restrict the availability of individual programs so that users can only see those that are authorized. NetTools ties in with NetWare Directory Services to restrict access to applications by userid, groupid, or other NDS information. Administrators can access any user-secured workstation through the use of an administrator's override password. NetTools provides broadcast and alarm alerts.

In addition to selecting a monitoring and reporting product, a sniffer, and perhaps a Windows management product from those described above, two additional specialized products are recommended: a password cracker and an application that automatically logs off inactive terminals. E.G. Software produces SmartPass NLM, a password cracking NLM for NetWare administrators. SmartPass examines user passwords against a database of 150,000 weak passwords (much larger database than KSA) and notifies the NetWare administrator of accounts with weak or nonexistent passwords. The administrator then informs the users of the problem and, as proof, is able to show them their password.

NETInc. produces NetSentry, a workstation application for NetWare networks, that automatically logs off inactive workstations. The administrator can also identify key applications, users, and groups that should *not* be logged off when they are idle.

One other product worthy of mention is the Cisco Systems Internetwork Operating System which provides access control, encryption, call-back modem capability, and single-user security hardware/software in NetWare 4 and other environments. Cisco can be contacted at: 170 W. Tasman Drive, San Jose, CA 95134, (800) 553-6387.

3.5 Firewall Security

As will be discussed in **Section 4**, the connection of an organization's NetWare network to external networks such as the Internet provides enormous opportunities for gathering and distributing information. Connections to Internet also introduce opportunities for adversaries to access the organization's information resources. The purpose of Internet connectivity is often to take advantage of electronic mail and file transfer using protocols such as Simple Mail Transfer Protocol (SMTP) and File Transfer Protocol (FTP). Unfortunately, these protocols include features that can be taken advantage of by an outsider to gain access to the internal network and attached servers. For example, FTP can be used for command submission to issue Unix commands unless action is taken to prevent such access. Since there is no standard on which port the various applications must use, implementations are not uniform and vendors often implement different ports for undocumented proprietary use. Furthermore, some protocols introduce undocumented capabilities that may not be protected against by the administrator and may be discovered by the outsider.

A firewall is a protective barrier that attempts to prevent passage of unauthorized traffic between the internal subnetwork and the external internetwork. There are many varieties of firewalls, some of which are very easily penetrated while others are more secure. The strategy should be to implement a firewall that does not allow application protocols to "tunnel" through the firewall to an address on the internal network, but to terminate the connection at the firewall and relay the information in a new connection between the firewall and the internal host. This is accomplished by an Application Gateway Firewall. Another strategy is to disable protocols that are not needed and to turn off ports not specifically needed by the authorized protocols.

The NOV*IX for Internet NLM by Firefox, listed in **Table 3-5**, is an Application Gateway Firewall specifically designed for NetWare. NOV*IX allows the network to be configured with only one Internet Protocol (IP) address for the entire organization so that all traffic to the organization must terminate at one host, the firewall. This is accomplished using the NOV*IX IP-IPX Transport Relay which converts Internet IP packets to NetWare IPX/SPX packets, and vice versa. This approach not only enhances security, but it eliminates the need for TCP/IP protocol suites to be installed on internal hosts. The only problem with this model is that the NOV*IX server is also the NetWare server rather than a dedicated server. If an attack mounted against the firewall should succeed, the adversary would have penetrated the NetWare server. The firewall may also be designed with IP addresses being assigned to specific servers (such as SMTP servers, FTP servers, and World Wide Web servers), or to individual NetWare users or groups if the administrator determines a need. NOV*IX includes a domain filter based on domain naming which permits the NetWare administrator to manage user access based on userid or groupid and NetWare security rights associated with those objects. The NOV*IX SMTP/POP (post office protocol) Mail NLM is an application filter for inbound mail. The Network News Transfer Protocol (NNTP) filter is an example of an outbound filter that controls access by insiders to news groups on the Internet. NOV*IX Host Connection Management includes trace/diagnostic capabilities that let the administrator produce protocol analyzer type traffic analysis of packets. The utility also includes an audit trail and audit reduction tools to assess activity. There is also a real-time connection monitor which provides a snapshot of current activity. Firewall management is complex and error prone. NOV*IX uses NetWare interfaces and NDS rights to streamline the process. Users of NOV*IX say that it's ease of use is it's biggest benefit. NOV*IX can be combined with other products for an even stronger firewall. It can also be used by dial-up users with IPX on their workstation (but not the TCP/IP suite) to connect to Internet.

Teltrust.com provides the WiseNet Service to give NetWare GroupWise users with electronic mail access over Internet. Teltrust.com "guarantees" that their clients business cannot be hacked through WiseNet's firewall. This may be an alternative to installing a firewall for more serious connectivity to Internet.

The Sidewinder by Secure Computing Corporation is a robust Application Gateway firewall, but it is not specifically designed for NetWare. All internal IP addresses are translated into a single IP address so that all outbound traffic appears to originate from a single IP address, that of the Sidewinder, to hide internal addresses. The Sidewinder firewall has application proxies for SMTP mail, Network News Transfer Protocol (NNTP news), FTP, Domain Name System (DNS), World Wide Web (WWW), Gopher, and Telnet. Internet Control Message Protocol (ICMP) echo, Domain Information Gopher (DIG), traceroute, and nslookup are only supported for use by the administrator. The Sidewinder does not support Network Time Protocol (NTP) which is needed by some internal servers to synchronize with the outside world. It also does not support high-risk protocols such as Network File System (NFS), X-11, r-commands, or Internet Relay Chat (IRC).

Table 3-5. *Firewalls*

Product	Vendor	Features	Related Products
NOV*IX for Internet NLM	Firefox, Inc. 2841 Junction Avenue Suite 103 San Jose, CA 95134-1921 (800) 230-6090	- Specifically designed for NetWare - Address and port filtering - Domain name filtering - Circuit filtering - Application filtering - IP-IPX Transport Relay - Connection stops at firewall - Protocol analyzer and report generator	- NOV*IX SMTP/POP Mail NLM - Host Connection Management - NOV*IX Transport Relay - NOV*IX Firewall Management - NOV*IX Domain Filter - NOV*IX Application Filter - Internet Connection Security (ICS) - Remote Connect Security (RCS)
WiseNet	Teltrust.com 5520 W. Harold Gatty Dr. Salt Lake City, UT 84116 (800) 826-4666	- E-mail for Novell GroupWise users - "Guaranteed" to be unhackable	–
Sidewinder	Secure Computing Corp. 2675 Long Lake Road Roseville, MN 55369 (800) 700-8328	Application Gateway Secure domains for each application	Authentication server Challenge-response mechanisms
CyberGuard	Harris Computer Systems Corp. 2101 W. Cypress Creek Ft. Lauderdale, FL 33309 (800) 245-6453	Application Gateway B-1 certified	–
BorderWare Firewall Server (BFS)	Border Network Technologies, Inc. 1 Yonge Street, Suite 1400 Toronto, Ontario Canada M5E 1J9 (800) 334-8195	Application Gateway	–
SmartWall	Virtual Open Network Environment Corporation 12300 Twinbrook Pkwy Suite 235 Rockville, MD 20852 (301) 881-2297	Application Gateway - One-time password - Single sign-on	- SmartCAT (smart card) - Smart CAT-EC (electronic commerce)

The Sidewinder's administrator interface is menu driven and easy to use. Its access control rulebase allows the administrator to designate which applications will be allowed to pass traffic through the firewall, which direction they be allowed (generally only outbound access, except for news and mail), and which source and destination addresses will be allowed to use each application. Options for challenge-response authentication will be available for various applications this year. The audit trail can be configured to capture events involving probe attempts to unsupported ports or services, attempts to access unauthorized files, and attempts to access services that are not authorized for the source address attempting to use the service. Alarms can be set to log the events to audit trails and printers, send e-mail messages to designated administrators, and send alerts to pagers. While the Sidewinder is not being designed specifically for military purposes, its design is based on that of the Secure Network Server which is being developed to meet A-1 criteria under the Multilevel Information Systems Security Initiative (MISSI).

The CyberGuard by Harris Computer Systems Corporation is similar to the Sidewinder in that it is an Application Gateway firewall which proxies connections so that internal hosts are not connected directly to external hosts. The CyberGuard supports all of the applications that the Sidewinder supports plus NTP, ICMP, and finger. It has a similar user interface, audit trail, and alarm capability. The CyberGuard runs under the Night Hawk operating system which has been formally evaluated by the National Computer Security Center at the B-1 level and may be appropriate as a firewall between departments within a military organization.

The BorderWare Firewall Server (BFS) by Border Network Technologies, Inc. is another robust firewall with packet filtering and application filtering that is not specifically designed for NetWare. As with Sidewinder and CyberGuard, all internal IP addresses are translated into a single IP address by the BorderWare firewall. The BorderWare Firewall Server has applications for SMTP mail, POP mail, NNTP news, FTP, DNS, WWW, Finger, Telnet and FTP Proxy to internal hosts, and Telnet, FTP, WWW, and Gopher proxies to external hosts. Inbound proxies require DES based challenge-response authentication. An audit trail is kept for all connection requests and server activity. Alarms can be configured to trigger e-mail, pop-up windows, printouts, and halt the system.

Another application level firewall is the SmartWall by Virtual Open Network Environment (V-ONE) Corporation. SmartWall operates under Windows and includes gateway proxies for FTP, SMTP, NNTP, WWW, Telnet, rlogin, and Secure Telnet. It performs challenge-response and mutual challenge-response authentication, and encryption of files, directories, and sessions. Another V-ONE product is the SmartCat smart card authentication mechanism using Smart Card Token Management which includes a digital photo and fingerprint biometrics, and S/KEY one-time passwords.

Other firewalls which are not specifically designed for NetWare environments, but which appear to provide application filtering and proxies, challenge-response authentication, one-time passwords, auditing, response to detected intrusion, and encryption include:

- *Gauntlet* – Trusted Information Systems, Inc., 3060 Washington Rd., Glenwood, MD 21703, (301) 854-6889; related products include TIS Internet Firewall Toolkit

- *The Eagle Enterprise System* – Raptor Systems, Inc., 69 Hickory Drive, Waltham, MA 02154, (800) 932-4536; related products include Eagle Remote (for remote offices) and Eagle Lite (for companies with 100 or fewer Internet users)

- *SecureConnect* – Morning Star Technologies, 3518 Riverside Drive, Suite 101, Columbus, OH 43221-1754, (800) 558-7827

- *Two Secure Routers + Bastion Host System* – Firewall Security Corporation, P.O. Box 35567, Monte Sereno, CA 95030, (408) 983-4901; related products include Authentication Server and Bastion Host System

- *ANS InterLOCK* – ANS CO+RE Systems, Inc., 1875 Campus Commons Drive, Suite 220, Reston, VA 22091-1552, (800) 456-8267

- *Screening External Access Link (SEAL)* – Digital Equipment Corporation, 146 Main Street, Maynard, MA 01754, (508) 496-8626 or (800) 354-9000 for general information.

Besides installing a firewall, it is important to test the firewall. One method is to attempt to penetrate the organization from the Internet. There are consulting companies that can help accomplish penetration analyses. There are also tools available for this purpose. One such tool, called the Security Administrator Tool for Analyzing Networks (SATAN) by Pilot Network Services, Inc., has been very controversial because it was distributed freely over the Internet. Many fear SATAN will be used by hackers to intrude into organizations they might have otherwise not been able to penetrate. Supporters feel that hackers will have similar tools anyway, and SATAN can be used by administrators to evaluate their own firewall and fortify where vulnerabilities are found. Currently, the platform base that SATAN will run on is limited. Descriptions of SATAN can be retrieved from `http://192.197.56.11/docs/Satan_doc.html` or `www.cs.ruu.nl/cert-uu/Satan.html` or any of dozens of other locations. The source code can be retrieved from `ftp://ftp.win.tue.nl/pub/security/satan_doc.tar.Z` or `ftp.sgi.com/pub/Satan/extra_programs/ftping.<platform desired>.exe.tar.Z`. If you choose to use SATAN, be sure to use version 1.1.1 or later because earlier versions introduced a vulnerability associated with the use of Worldwide Web.

To help combat SATAN by alerting the administrator when a SATAN attack is being launched on a system, a tripwire application, called *Courtney,* has been developed. Courtney is available free at `http://ciac.llnl.gov/ciac.ToolsUnixNetMon.html#Courtney`. There is also code recommended by Morning Star Technologies for installation on the firewall to help block many SATAN attacks, or at least confuse the adversary and make it inconvenient to persist in the attack. Morning Star's recommendations are available at `http://www.MorningStar.com/mst-satan.html`.

3.6 Virus Protection

There are two key ways in which an administrator can use NetWare security to protect against virus attacks: limit the right to modify an executable file; and create a pseudo-supervisor to minimize use of the main supervisor account [BAKER 95]. Network administrators have recognized the importance of additional protection, installing more antivirus products than products for any other security area. Due to this demand, there are many excellent antivirus products specifically designed for NetWare. The most common approach used in these products is to scan for viruses that already exist on the system. This is done by searching for virus code string signatures or by using rule-based algorithms. Monitoring for virus-like behavior (e.g., writing directly to the hard disk, terminating and staying resident, attempting to change executable files or file attributes) and scanning files as they enter the server or at least before they execute helps to prevent the spreading of viruses. Prevention techniques include not allowing users to write to certain disks, directories, system files, and boot tracks. Some antiviral products calculate cyclic redundancy checks (CRCs) against the files and store the CRCs as fingerprints for future validation of integrity. Virus protection NLMs can sanitize the server, keep unprotected workstations from logging onto the network, and monitor the network to locate and isolate sources of virus outbreaks.

When selecting the appropriate product, the NetWare administrator should consider whether the product is an NLM, whether it protects both the NetWare server and the workstation, and whether the product runs in real-time, scanning files as they are being transmitted to the server in order to stop the virus from spreading further. The products recommended in this section and listed in **Table 3-6** meet these criteria.

Novell's ManageWise (discussed in **Section 3.4**, Network Analysis and Management) has a good virus protection product – the LANDesk Virus Protect NLM by Intel Corporation. LANDesk Virus Protect NLM can be configured centrally to check all servers and workstations in the enterprise-LAN, automatically logs into the Intel bulletin-board system (BBS) periodically to download updated virus pattern files, has excellent auditing and reporting capabilities, has excellent alert capabilities including broadcasts to the workstation or server console and alerts the administrator when the workstation is logged out, can send alerts via e-mail, scans Macintosh files, and can scan some compressed files. Weaknesses are that the user interface is not as good as other products and file integrity checking is not performed against previous versions.

Central Point Anti-Virus for NetWare NLM, by Symantec Corporation (previous developed and marketed by Central Point Software), is a full-feature NLM and workstation product which may be the best enterprise-wide anti-virus system. Central Point has an excellent user interface and help system and coordinates protection across servers. Central Point automatically updates periodically with new virus patterns, has excellent auditing and reporting capabilities, has excellent alert capabilities including broadcasts to the workstation or server console and alerts the administrator when the workstation is logged out (so long as the LAN drivers remain installed), can send alerts via e-mail or dial a beeper, scans Macintosh files on both the server and the workstation, and performs integrity checks of files on the workstation.

Table 3-6. *Antivirus Products*

Product	Vendor	Features	Related Products
Novell ManageWise with Intel Corporation's LANDesk Virus Protect NLM	Novell 122 E. 1700 South Provo, Utah 84606 (800) 453-1267 Intel Corporation (800) 538-3373	- Enterprise-wide - Automatic updates - Excellent audit & reports - Alerts broadcast & e-mail - Scans Macintosh files - Scans compressed files	–
Central Point Anti-Virus for NetWare NLM	Symantec Corp. Central Point Division 15220 NW Greenbriar Pky Suite 150 Beaverton, OR 97006 (800) 278-6657	- Enterprise-wide - Automatic updates - Excellent user interface - Excellent audit & reports - Broadcasts alerts, or via e-mail or beeper - Scans Macintosh files - File integrity checking	- Norton's Antivirus for NetWare NLM (different division of Symantec)
Norton's Antivirus for NetWare NLM	Symantec Corp. 10201 Torre Avenue Cupertino, CA 95014 (800) 441-72343	- Enterprise-wide - Novell approved for 4.1 - Automatic updates - Excellent audit & reports - Alerts broadcast & e-mail - Scans Macintosh files - File integrity checking - Can suspend scanning	- Norton's Desktop Network Menuing Administration Pack (encryption)
NET-PROT NLM	Command Software Systems, Inc. 1061 E. Indiantown Rd. Suite 500 Jupiter, FL 33477 (800) 423-9147	- Enterprise-wide - Very fast - Automatic updates - Mediocre audit & reports - Broadcasts alerts - Scans compressed files - File integrity checking - Can suspend scanning	- F-PROT Professional (for the workstation)
InnocuLAN NLM	Cheyenne Software 3 Expressway Plaza Roslyn Heights, NY 11577 (800) CHEY-INC	- Enterprise-wide - Novell approved for 4.1 - Automatic updates - Audit & reports - Broadcasts alerts, or via e-mail, fax, beeper - Scans Macintosh files - Can suspend scanning	–
NetShield NLM	McAfee, Inc. 2710 Walsh Avenue Santa Clara, CA 95051 (800) 866-6585	- Enterprise-wide - Automatic updates - Audit & reports - Broadcasts alerts - Scans compressed files - Can suspend scanning - Can purchase off BBS	- VIRUSCAN (client for workstations)

Central Point Software was recently bought out by Symantec; Symantec continues to market Central Point Anti-Virus for NetWare, but will likely merge the best features into their Norton's Antivirus for NetWare NLM and cease to market Central Point. Symantec states that Central Point customers will be permitted to upgrade to Norton's if Central Point is taken off the market.

Norton's Antivirus for NetWare NLM, by Symantec Corporation, is another excellent product which is approved by Novell as an NLM for NetWare 4.1. It has an excellent user interface and help system, updates server antivirus files automatically (but not the workstation), has excellent auditing and reporting capabilities, has excellent alert capabilities including broadcasts to the workstation or server console, can send alerts via e-mail, scans Macintosh files, performs file integrity checks, and can suspend scanning during peak system loads to improve performance. Norton's was not as fast as NET-PROT NLM (discussed below) in testing by the National Testing Software Laboratories, but is faster than most other antiviral products [NTSL 93].

NET-PROT NLM, by Command Software Systems, Inc., is a full-feature NLM and workstation product which runs faster than any other product discussed here (a significant feature of an NLM), is also an enterprise-wide system, and is listed by Novell as an approved NLM for NetWare 4.1, but is not quite as user friendly. NET-PROT automatically updates periodically with new virus patterns, has alert capabilities including broadcasts to the workstation or server console, can scan some compressed files, performs integrity checks of files on the workstation, and can suspend scanning during peak system loads to improve performance. It has auditing and reporting capabilities but saves the files only in ASCII format and cannot print audit reports from the program.

InnocuLAN NLM, by Cheyenne Software, is another NLM approved by Novell for NetWare 4.1. InnocuLAN automatically updates periodically with new virus patterns, has alert capabilities that include broadcasts to the workstation or server console, can send alerts via e-mail, fax or beeper, has auditing and reporting capabilities, scans Macintosh files, and can suspend scanning during peak system loads to improve performance. Drawbacks are that InnocuLAN is a memory hog and is relatively slow, though it has had strong user acceptance.

Finally, NetShield NLM, by McAfee Inc., is another full-feature NLM and workstation product which is well suited for an enterprise environment. NetShield automatically updates periodically with new virus patterns, has alert capabilities that include broadcasts to the workstation or server console, has auditing and reporting capabilities, scans some compressed files, and can slow scanning during peak system loads to improve performance. As with InnocuLAN, drawbacks are that NetShield is a memory hog and is relatively slow, but it also has had strong user acceptance. McAfee has acquired SunSoft Inc. (network security management), Brightwork Development Inc. (server based LAN management), and products from Automated Design Systems, Inc. (Net Tools and Help+) and McAfee is committed to producing top-of-the-line products, including NetShield. A nice feature is that NetShield can be downloaded from the McAfee BBS and be paid for when it goes into production.

This Page Intentionally Left Blank

Section 4

External Interfaces

This Page Intentionally Left Blank

4.0 External Interfaces

Organizations that carry highly sensitive information on their LAN may be unable to consider the introduction of external access capabilities such as dial-up connectivity and gateways to the Internet. Other organizations that have LANs for the sharing of less sensitive information may find the risk of implementing such connections to be acceptable. This section acquaints the NetWare administrator with the issues at a high level and directs those that are interested to specific references which cover these topics in detail.

4.1 Connections to Internet and Other External Networks

Naval LANs provide interconnectivity throughout a department or entire organization. This interconnectivity includes electronic mail and file transfers. Some organizations also extend the interconnectivity to other organizations. The Internet is an interconnected worldwide collection of networks that any organization may connect to if they choose. Navy organizations have recognized that it is to their advantage to allow their staff to connect to the Internet in order to extend the electronic mail and file transfers beyond their local organization.

Many new Internet protocols and applications have been developed in the past year and more will be developed in years to come. Most notably, the World Wide Web is an application that uses non-linear hypertext (text with pointers off the page) and non-text hypermedia (text, graphics, and sound) to allow menus and files to point to other directories and files located anywhere on the Internet. Several workstation applications, in particular NETSCAPE (Netscape Communications Corporation), have been developed for browsing the 'Web'. There are also very fast search robots such as WebCrawler (University of Washington), World Wide Web Worm (Oliver McBryan, University of Colorado), and ALIWEB (Nexor, United Kingdom) that search for files containing keywords selected by the user.

The NetWare administrator must be aware of the trend toward interconnectivity and take steps to support this need, while at the same time taking steps to protect the organization from outside tampering. As discussed in NIST Special Publication 800-10 [NIST 94D], a *firewall* is needed to help protect the organization's LAN from unauthorized outside access. Another name for a firewall is *secure Internet gateway.* A firewall can be used to connect the organization's internal network to an external network and provide traffic routing services between the external and internal networks. It may also store information that the organization wishes to make public to the outside world (e.g., Web home pages and archives available for Anonymous FTP access). The traffic routing services may be implemented at the Network Layer by incorporating filtering rules in a router, or may be implemented at the Application Layer by using an Application Gateway as explained below. Each has advantages and disadvantages. Often the firewall will incorporate both approaches.

Until multilevel workstations are available and installed throughout the organization (meaning each workstation can provide full security for itself), a firewall is necessary to add access controls to the "front door" of the organization. However, firewall technology is immature and, as such, introduces risk. The NetWare administrator should not be lulled into a false sense of security that a firewall might bring. Firewalls are complicated and should be built by experienced networking experts. A firewall consists of a policy, hardware and software components, and management controls. The policy is vital and should not be overlooked. There are a wide variety of configurations, each offering benefits and drawbacks. Likewise, controls can be applied to a wide variety of protocols, each requiring careful consideration. If your organization lacks specific experience, the network administrator is advised to recruit a consultant to help design and install the first firewall and help monitor traffic and perform penetration studies during the burn-in period.

There are several flavors of firewalls. The most common, and by far the least effective, version is the *Packet Filtering Firewall* shown in **Figure 4-1**. This is sometimes also called a 'Screened Router' or 'Firewall Router'. Packet Filtering Firewalls simply block services (i.e., protocols) that are not needed. However, attacks can be launched using the protocols that are allowed through the firewall. Packet filtering is usually done by a packet filtering router designed for filtering on *sockets* which consist of Internet Protocol (IP) source and destination addresses (which identify the host computers for the connection) and Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination ports (which help to identify the application being used). There are many ways to defeat simple filtering designed to keep out traffic from unauthorized sources or unauthorized Internet applications. Even if the packet filtering router performs all filtering according to the rule set, which they have not been verified to do, there are inherent weaknesses in the Internet protocols.

For example, source routing allows a source to identify a path that the message will take to the destination and the response will take on the way back. If an adversary can determine a source that is acceptable to their target, they can send a message that appears to have originated from the acceptable source and has a source routing list that

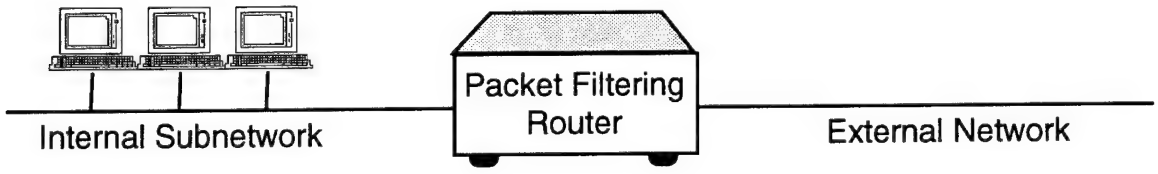


Figure 4-1. *Packet Filtering Firewall*

includes themselves. Thus, it is possible that the attacker is sending this message, and if so, it is assured that any replies will be returned to them, supposedly enroute back to the destination.

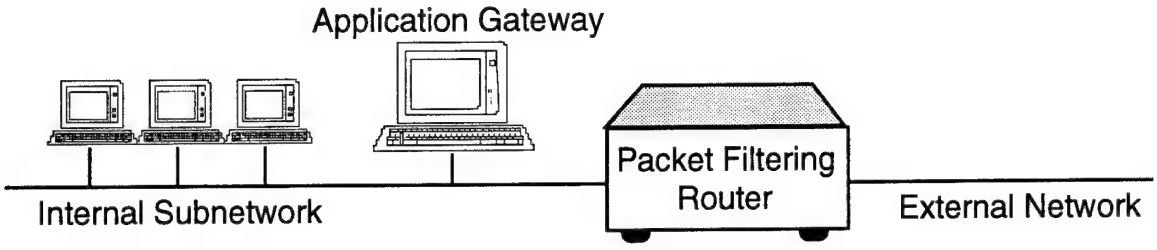
Even electronic mail, which most Navy personnel will want to use, is vulnerable. The protocol includes a Verify Postmaster command which, if not disabled, will return information (true name, etc.) about the postmaster of the organization. This information can be used to launch a directed attack against the postmaster's user account which is likely to have system privileges. Many mail programs also recognize Unix commands embedded in the header and will pass those commands to the operating system for execution! Users must not be permitted to use these programs if the organization is to be connected to Internet. Specifics on this topic are available in [CHES 94].

Additional weaknesses associated with Packet Filtering Firewalls are: filtering rules are difficult to test completely, often leaving unknown vulnerabilities; traffic that is permitted to pass through the filter is delivered to internal hosts where they may launch an attack; and little logging can be done on a router. Clearly, packet filtering does not provide sufficient protection for many environments.

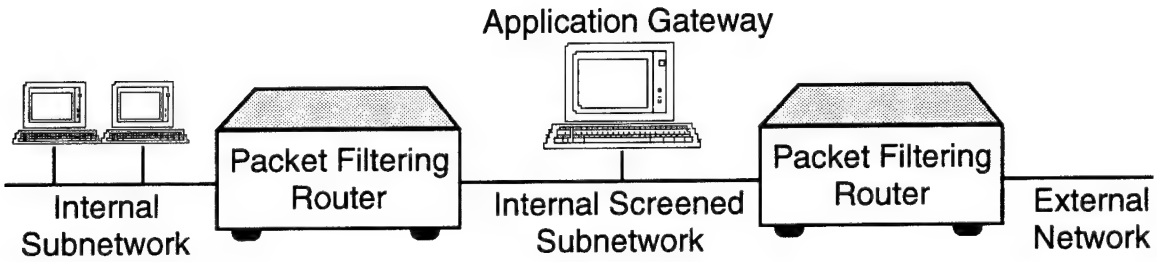
An Application Gateway is needed to intercept and terminate traffic and then act as a proxy to accomplish the communications task. There are several varieties of Application Gateways. The three most common, beginning with the least secure, are (a) *Screened Host Firewall,* (b)*Screened Subnet Firewall,* and (c) *Dual-Homed Gateway,* shown in **Figure 4-2.**

Each of the three configurations includes an Application Gateway which incorporates special-purpose programs to apply filtering and proxy services for desired applications. By using proxy services, the Application Gateway can actually act as the terminus of the external connection and then establish a proxy connection between itself and the internal host eliminating the possibility of the external agent acquiring access to the internal host, which is presumed to be less secure than the Application Gateway if for no other reason than the number of user accounts that exist on internal hosts. Application Gateways also have the ability to log all incoming and outgoing traffic. Of course, security of the Application Gateway itself is vital. The drawback to including an Application Gateway in the configuration is that the need for custom programs for each application will limit the ease with which applications can be implemented on the firewall. The added components also introduce additional possibilities for error in an already complex system.

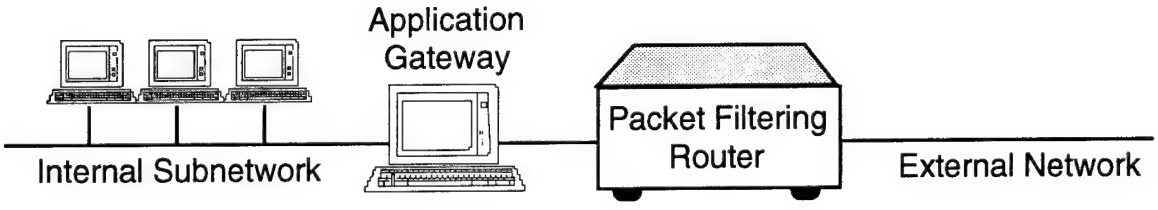
The advantage of the Screened Host Firewall configuration is that the Application Gateway can be connected to the existing internal subnetwork, minimizing cost. The packet filtering router forwards most incoming traffic to the Application Gateway for action, but is able to route "trusted" traffic directly to internal hosts. This allows protocols with known vulnerabilities to be processed by the Application Gateway while allowing relatively safe traffic (based on a judgment call be the NetWare administrator) to be handled in the same manner as a Packet Filtering Firewall would handle it.



(a) Screened Host Firewall



(b) Screened Subnet Firewall



(c) Dual-Homed Gateway

Figure 4-2. *Application Gateway Firewalls*

The Screened Subnet Firewall incorporates two routers and a second internal network to create an inner screened subnet on which the Application Gateway resides. An attacker would have to subvert both routers to reach internal hosts (this may be easy if the administrator uses default passwords or the same password on both routers). Besides the Application Gateway, communications and information servers can be placed on the screened subnet and be made known to external hosts. Another advantage is that routers process traffic faster than Application Gateways; thus, the Screened Subnet Firewall may be preferred over the more secure Dual-Homed Gateway for Sensitive Unclassified environments with large amounts of traffic.

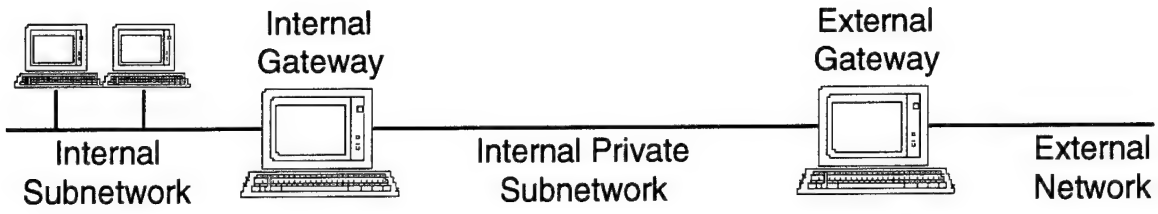
The Dual-Homed Gateway inserts an Application Gateway in the path of all traffic through the firewall. It cannot be bypassed. It is the most secure of the three shown because, first, all traffic must be processed by the Application Gateway and, second, services for which there is no proxy cannot be processed.

Still more complex Application Gateway Firewalls incorporate two Application Gateways (an inner and an outer) which do not even trust each other, as shown in **Figure 4-3(a)**, and a choke router to enforce a private link between the outer and inner Application Gateways, as shown in **Figure 4-3(b)**. While the first configuration is very secure, the second configuration can be attacked at either the outer Application Gateway or the Choke Router but is much faster (since routers process traffic faster than Application Gateways) and is often used with routers that filter on output only. When the outer Application Gateway is exposed to the external world (i.e., there is no packet filtering router in front of it), it is referred to as a *Bastion host.* Both of these configurations could be strengthened by adding a firewall router on the front side.

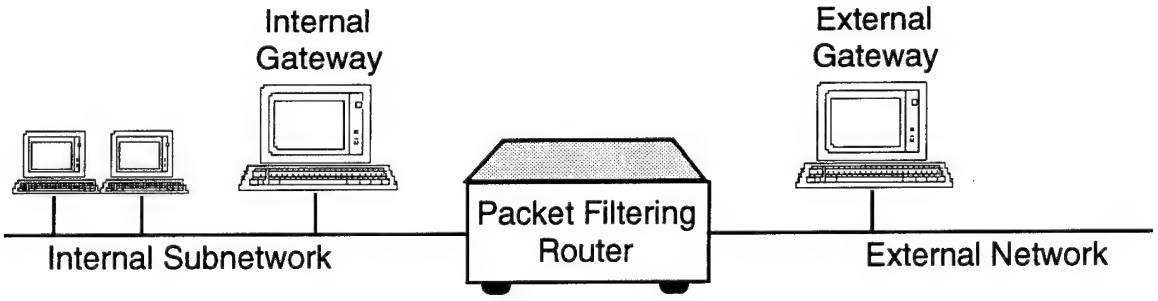
In addition to Packet Filtering Firewalls and Application Gateway Firewalls, there are *Circuit-Level Gateways.* [CHES 94] A Circuit Gateway relays TCP connections but does no extra processing or filtering of the protocol. It simply provides a relay service between the caller's connection to the gateway and the destination on the other side of the gateway. This may be preferred for outgoing connections where the bytes of traffic do not need to be examined once the connection has been established and traffic is flowing through.

A firewall will not solve all the interface problems. Many Internet protocols transmit passwords in the clear or introduce other security vulnerabilities; data is not typically encrypted for privacy; and of course, there are important issues associated with the administration of a firewall. There are many alternatives for addressing these issues. NIST recommends that organizations use advanced authentication measures, i.e., smart cards, or authentication tokens, or other one-time password mechanism, as an integral part of their firewalls for authenticating connections to site systems. [NIST 94D] Firewalls also do not protect against the downloading of virus-infected software from Internet archives or transferring such programs in attachments to e-mail. [NIST 94D]

For introductory information on firewalls, refer to [NIST 94D]. For a more comprehensive discussion of the topic, refer to [CHES 94].



(a) Dual Application Gateways



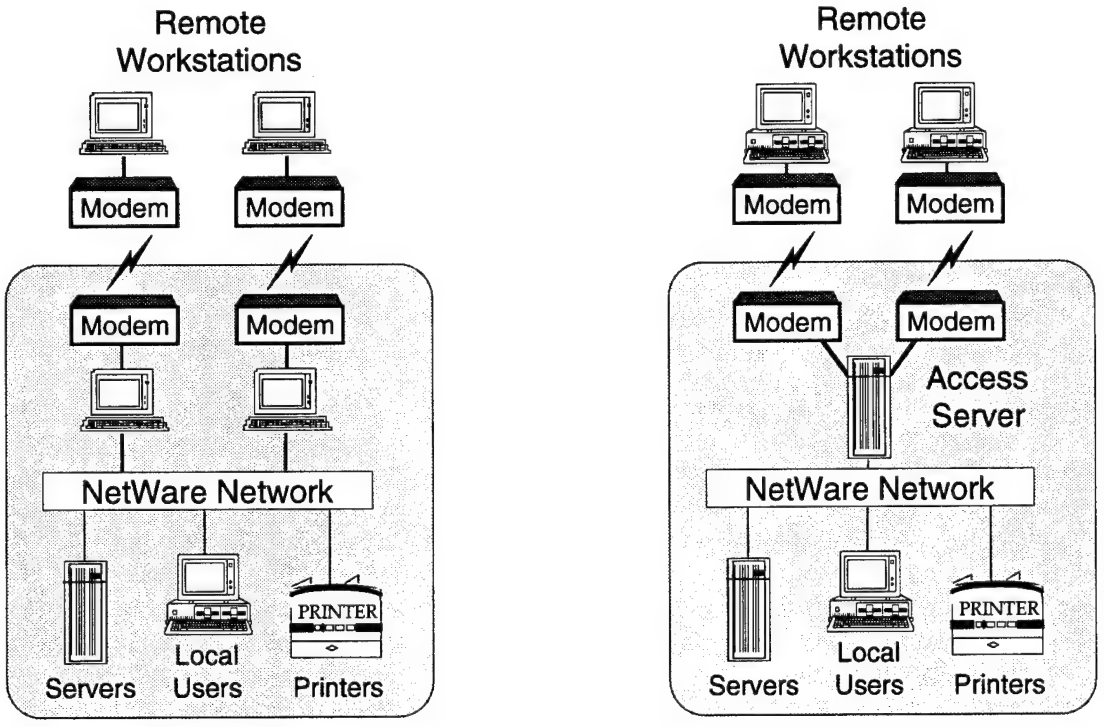
(b) Dual Gateways with Choke Router

Figure 4-3. *Complex Application Gateway Firewalls*

4.2 Dial-up Access

Organizations that consider connections to the Internet to be unacceptable due to a high level of risk may still determine that dial-up capabilities are acceptable, provided they are implemented in a manner that meets the security policy of the organization. Dial-up capabilities enable authorized users to access the systems when they are not on site even though Internet access is not available. However, dial-up capabilities introduce another avenue of approach for an intruder. A dial-up connection between a NetWare LAN and a remote workstation or other network can be made using telephone lines and modems, enabling connections over greater distances than normal cabling would permit. A modem converts digital signals to analog signals and vice-versa to enable computers to send information across telephone lines.

There are two possible configurations for providing dial-up access to NetWare networks: Remote Access Connections and Direct Dial-up Connections, as shown in **Figure 4-4**. In the case of remote access connections, the remote access software treats the remote workstation as a dumb terminal and performs all computing tasks on workstations connected to the NetWare network. [SHELDON 94] Only screen and



(a) Remote Access Connections **(b) Direct Dial-up Connections**

Figure 4-4. *Dial-up Connections*

keyboard information is transmitted, and file transfers are not possible. The drawback is that dedicated computers are required to service each dial-in user. The second option connects dial-up users directly to the network as if they were connected locally. This increases the security risk as well as the traffic load. In this configuration, most processing should be done from the remote workstation rather than from the network.

Modem gateways can and should be used to pool the modems for sharing by all dial-up users. This reduces the cost by not requiring a modem for each host on the network and it also increases security by consolidating all modems into a single location where they can be managed and controlled more effectively.

A variety of Novell and third-party remote access software is available for NetWare environments. Some are optimized for Windows and client-server applications. [SHELDON 94] Examples for remote access connections include Carbon Copy from Microcom, Close-Up from Norton-Lambert, and Norton pcANYWHERE from Symantec Corporation. An example for direct dial-up connections is Novell's *NetWare Access Server* which includes a dial-back feature that helps ensure the caller is calling from a location that is known and approved by the administrator.

Novell's *NetWare Connect* is a communications server that lets mobile (i.e., wireless) users connect to NetWare networks. It provides remote node, remote control, dial-in and dial-out services, and security and management features. Microsoft is developing features in Windows that automatically restores a user's work environment so the user can disconnect at one location and reconnect at another without losing their setup or work. [SHELDON 94] Remote access is becoming a necessity in many environments. The NetWare administrator must consider security options for enabling the dial-up capability while reducing the associated risk to an acceptable level.

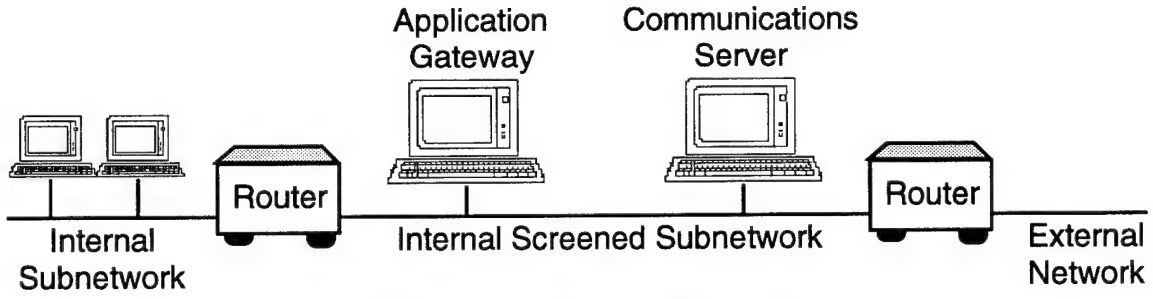
As discussed in **Section 2.6**, the NetWare server console can be accessed by the administrator from any workstation, including dial-up workstations, using the REMOTE and RCONSOLE utilities. REMOTE enables remote connections and RCONSOLE allows remote server console actions including: using console commands as if they were entered from the server console, scanning directories and editing files on a server, transferring files to (but not from) a server, shutting down a server, and installing or upgrading NetWare on a remote server.

REMOTE also enables users to encrypt their password. *The use of this feature is strongly recommended, particularly for privileged users such as the NetWare administrator.* In addition, NetWare includes the NetWare Remote Management Facility (RMF) which allows the NetWare administrator to install and upgrade NetWare, configure network services, and maintain NetWare from a remote workstation.

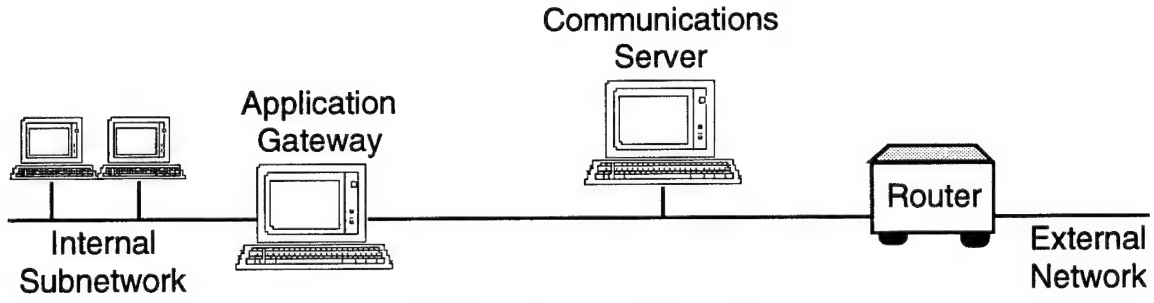
Refer to [NOVELL 94U] for detailed explanations of the installation and use of REMOTE, RCONSOLE, RSPX, RS232, and AIO that are required for using RCONSOLE over a dial-up line, encrypting the password, and creating a callback list.

4.3 Combining Firewalls and Communications Servers

When possible, the dial-in *and dial-out* capabilities should be designed into the firewall and the connection of modems to internal hosts should be prohibited. Examples of how the modem pool can be built into the firewall are shown in **Figure 4-5** below. In both examples, all modems are connected to the communications server. The communications server is protected from Internet access to some degree by the Packet Filtering Router. All incoming and outgoing traffic, whether it originates from an internal host, a dial-up host, or over the Internet, must be processed by the internal Packet Filtering Router or, better yet, the Application Gateway. If an Application Gateway is included in the configuration, it would process traffic for any connections between the communications server and the Internet.



(a) Screened Subnet Firewall



(b) Dual-Homed Firewall

Figure 4-5. *Placement of the Modem Pool*

This Page Intentionally Left Blank

Section 5

Residual Vulnerabilities

This Page Intentionally Left Blank

5.0 Residual Vulnerabilities

NetWare 4 has many more security features than did NetWare 3, and NetWare 4 is easier to administer. Still, NetWare 4 does not provide all of the capabilities for protecting information that may be desired in some sensitive environments. As was seen in **Section 3**, third-party vendors provide many of those desirable capabilities. At the same time, these products make the environment more complex and more difficult to manage; and even with the add-on products, vulnerabilities will continue to exist. The residual vulnerabilities discussed in this section can be minimized with careful and complete management. Partial solutions to each vulnerability are also discussed.

5.1 Workstation Security and User Security Awareness

The most common source of security problems is the lack of training or the lack of concern among the user community. In a mainframe environment, administrators often enforced security practices over the objections of users. In a distributed client-server environment, users have more of a feeling that control of the workstation is their responsibility, not the network administrator's. Some will not understand or comply with a policy that prohibits the use of unauthorized software, modems, and other add-on products. A comprehensive employee security awareness training program is vital in order for the NetWare administrator to enlist the user community in helping support the organization's security policies. Employees need to be educated and reminded as to the criticality and sensitivity of their data, the risks that exist in a networked environment, and the precautions that are necessary to safeguard their data.

5.2 Balanced Administration

Where organizations typically had backup administrators for their mainframe environments, that is not the case for client-server environments, but it ought to be. The information being processed in a distributed environment is the same information that was processed in the centralized mainframe environment and it has the same criticality and sensitivity as before. Therefore, it requires the same level of security. Administrative duties and responsibilities should be shared by more than one person. Not only does this implement a form of checks and balances, but it reduces the number of network components and objects that the individual administrator must manage, making it less likely that errors will occur. It also provides a mechanism for training backups to replace key personnel who leave the organization.

The Auditor Role should be assigned to a second party to review the security controls (e.g., user rights, administrator rights, password restrictions, auditing) implemented by the administrators. Network administration is complex and error prone. Auditors support the administrators by identifying weaknesses in the security structure of the network. Administrators can also turn off security mechanisms in the interest of higher processing rates. It is the auditor's responsibility to perform unannounced audits to detect these deficiencies and take action to have them corrected.

5.3 Network Components

Firewalls, routers, bridges, and hubs all have management software that enforces the security rules of the organization. Most components implement the Simple Network Management Protocol (SNMP) which allows the device to capture and read packets for the purpose of routing and filtering, though user data can be read as well. SNMP can also activate on-line alarms in the event of damaged or erroneous packets or security violations. These controls can either be accessed through the console attached to the device or over the network. Three safety precautions are important. First, network components should be housed in secure environments, such as what is provided for the NetWare servers. An adversary who can gain control of a network component can intercept user data and acquire userids and passwords for both users and administrators. Second, administrators must make proper use of the access controls built into the network components, just as they do for NetWare servers. Administrators tend to neglect component security by using passwords that are easily cracked, by leaving the passwords set to their defaults, by setting the passwords for all network components to the same password, and by turning off the audit trails. Third, if the network components are configured to allow administrator access over the network, specific network administration addresses should be assigned and attempts to access the component from any other network address should be denied and logged. All failed login attempts should be logged and tracked as well. Careful administration of the network components is extremely important.

5.4 Database Management Systems

Some database management systems (DBMSs) have the potential for introducing several exposures to risk. First, access rights to views of the database are defined and enforced within the DBMS, not within NetWare. Thus, coordination is needed between the DBMS administrator and the NetWare administrator to uniformly enforce the organization's security policy. Users' access rights within the DBMS should be reviewed to verify that their access authorities are consistent with their job responsibilities.

Some DBMSs allow users to connect directly to the application without using operating system sign-on security. While NetWare has fairly robust access controls, the DBMS may not have adequate access controls. This may be a concern because many applications define their database tables as "public" and any user that can sign on directly to the DBMS can read and update the tables regardless of the views that are assigned. If there is a choice, the administrator should impose NetWare access controls on the DBMS.

Some third-party products (e.g., SQLWindows by Gupta Technologies, Inc.) have the ability to access DBMS files without being authenticated by the DBMS access control mechanisms. This allows the user to dynamically upload and download information and generate reports without restrictions. NetWare administrators should control what programs are loaded onto the workstations and NetWare servers to prevent abuses.

5.5 Passwords "In The Clear"

While NetWare encrypts passwords during transmission within the organization's subnetwork, connections to external networks may use protocols that do not include password encryption. Any "X" type product, for example, is not likely to encrypt the userid or password, nor are most of the TCP/IP protocols used over Internet. Users that access applications on external networks should be advised to use different passwords than what is used within NetWare. The use of time-based or challenge-response authentication mechanisms are also recommended to help prevent outsiders from masquerading as authorized users. However, these mechanisms only work when the remote stations are equipped with cooperating mechanisms.

5.6 Dial-Up

Modems provide links for outsiders to access the organization's network. Unauthorized modems attached to workstations introduce an avenue of attack that may not be protected by NetWare or the communications server. Modems should be pooled at the communications server and access to the network should be prohibited via modems connected to workstations. Modems connected to network components (e.g., hubs, routers, gateways) are of particular importance because they have the ability to capture all traffic on the network. In addition, if the network configuration includes a firewall, the communications server should be incorporated into the firewall so that hackers who penetrate through the modems are no closer to the organization's subnetwork than are outsiders attempting to penetrate through an external network connection. An assessment of the criticality and sensitivity of the data should dictate whether strong authentication mechanisms, such as challenge-response authentication via smart cards, are also needed on the dial-up ports.

5.7 Leased Lines

Organizations which are geographically disbursed may incorporate leased lines into their architecture for connectivity between sites. These lines may use Integrated Services Digital Network (ISDN) circuits for 56 Kbps and 128 Kbps speeds, Switched Multimegabit Data Service (SMDS) for T-1 and T-3 speeds (1.5 Mbps and 45 Mbps, respectively), or Broadband Integrated Services Digital Network (B-ISDN) for STS-3 and STS-12 speeds (155 Mbps and 622 Mbps, respectively). Since these channels provide private virtual circuits and are not usually shared with other organizations, the administrator may be lulled into a false sense of security. Even though the channels are not shared, they are provided by public carriers and are routed through the carrier's switches. Thus, they are may be intercepted. If the organization is processing highly sensitive information, end-to-end encryption may be in order.

5.8 Disaster Planning

Contingency planning has long been a major consideration in centralized environments. The redundancy that is inherent in a distributed environment reduces the risk of a catastrophic loss that may occur due to hard disk failures, fires, or other natural disasters. Nevertheless, the administrator should ensure that there is a current contingency plan for recovery in the event of a catastrophic event.

Section 6

Conclusions and Recommendations

This Page Intentionally Left Blank

6.0 Conclusions and Recommendations

Most security practices are common sense, but they do take planning, training, research of new products, testing, and a constant vigil. The distributed environment is an exciting architecture that has been defined as the "third revolution" shaping the world, the first two being the invention of the printing press and the industrial revolution. But interconnectivity also reshapes the risk factors, making information systems more secure in some respects and less secure in others. For example, the risk of catastrophic loss has been reduced in the distributed environment, but the risk of an adversary having an opportunity to penetrate the network has been increased.

The administrator that disables user controls, audit trails, virus checkers, and other security mechanisms is shooting themself in the foot. With the ever-increasing interconnectivity to external networks, consideration must be made for stronger authentication, encryption, network analysis tools, firewalls, and virus protection.

This handbook reviewed the Novell NetWare environment and suggested measures that the administrator should consider in order to provide adequate security for the information being processed by the organization. The conclusions and recommendations of this handbook are as follows:

- Security Posture – It is important that the security staff understand the threats and vulnerabilities of the system in order to reduce security risks to an acceptable level. This is accomplished through performance of a risk assessment. An important part of the risk assessment is the quantification of the sensitivity and criticality of the information to be protected. Decisions concerning the appropriate level of security to be implemented can only be made after determining the sensitivity and criticality of the data.

- NetWare Administrator Training – An overview of the NetWare NDS and File System structures was presented in **Section 2.** While this will acquaint the administrator with the concepts, in-depth training on NetWare administration is required. This can be acquired from authorized Novell trainers, or when that is not possible, video training is available from several sources. Administrators should continue to attend NetWare training courses to broaden their exposure to aspects beyond basic administration. Personnel who will perform NetWare Auditor roles should also attend training courses. Participation in user groups is recommended to provide contacts among peers for the exchange of ideas and recommendations.

- Implemention of NetWare Security Features – The security administrator is responsible for enforcing the organization's security policy. Guidance concerning the implementation of NetWare security features was presented in **Section 2.** Administrators should carefully review these recommendations and consider whether they are appropriate for their organization. They should also understand the concepts so that they can modify their implementations as necessary. Once the mechanisms have been activated, they should be tested and periodically

retested. Even experienced administrators make errors. Tools are available to assist in the analysis. They can identify vulnerabilities that would not have been found had the tools not been used. Protocol analyzers and network management products should be mandatory elements of the administrator's toolkit.

- Implementation of Secure External Interfaces – Organizations that are considering installing modems for dial-up access or gateways to external networks face increased risks from many sources. These risks can be managed with the right tools. **Section 3** discussed some of the concerns and presented an overview of firewall technology. The criticality and sensitivity of the information must be well understood before a decision to permit dial-up access or connectivity to external networks can be made. Firewall technology has improved dramatically in the past year, yet there are those who still feel any firewall can be penetrated and a firewall only provides a false sense of security.

- Use of Third-party Products – NetWare was not designed to provide a high level of security. Accordingly, the security features of NetWare are limited. Third-party products are available to the administrator that has a need for them. **Section 4** discussed products that enhance workstation access controls, provide stronger authentication than what is delivered with NetWare, provide data encryption for privacy, augment the administrator's analysis and management toolkit, implement firewalls of varying strengths, and provide virus protection. Many of these products are relatively inexpensive and are strongly recommended. Others are more costly, yet provide such strong degrees of security that they should be considered when the criticality or sensitivity of the data dictates.

- Employee Security Awareness Training – Any security program is doomed to fail if the user community is not educated, trained, and convinced of it's importance. Employee security awareness training that clearly describes the threat, purpose for the security policy, security policy, and user responsibilities is necessary in every organization.

Security is the responsibility of the entire organization from the top executive to lowest level clerk. The information belongs to every department, not just the data processing department. This concept has become better understood with the migration toward distributed systems. The security policy must originate at the top and encompass every department. Security awareness training must also encompass every department. The administrator is responsible for installing and maintaining mechanisms that support the security policy. In order to do an effective job of this, the administrator requires continuous training and contact with peers.

Appendices

This Page Intentionally Left Blank

Appendix A

Acronyms

This Page Intentionally Left Blank

Appendix A

Acronyms

ACL	Access Control List
ANSI	American National Standards Institute
API	Application Program Interface
ATM	Asynchronous Transfer Mode
BBS	Bulletin Board System
BFS	BorderWare Firewall Server
B-ISDN	Broadband Integrated Services Digital Network
CD	Change Directory
CNA	Certified NetWare Administrator
CNE	Certified Novell Engineer
CRC	Cyclic Redundancy Check
DBMS	Database Management System
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DNS	Domain Name Service
DOS	Disk Operating System
DQDB	Distributed Queue Dual Bus
DSS	Digital Signature Standard
FAQs	Frequently Asked Questions
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
Gbps	Giga (billion) Bits Per Second
GSS-API	Generic Security Service Application Program Interface
ICS	Internet Connection Security
ICV	Integrity Check Value
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPX	Internetwork Packet Exchange Protocol
IRF	Inherited Rights Filter
ISC	Information Security Corporation
ISDN	Integrated Services Digital Network
ITSEC	Information Technology Security Evaluation Criteria
KSA	Kane Security Analyst
LAN	Local Area Network
LCD	Liquid Crystal Display
LEAF	Law Enforcement Access Field
MB	Mega (million) Bytes
Mbps	Mega (million) Bits Per Second
MHS	Message Handling System
MSP	Message Security Protocol
NCSA	National Center for Supercomputing Applications

Appendix A – Acronyms (continued)

NDS	NetWare Directory Services
NEU	Network Encryption Unit
NIST	National Institute of Standards and Technology
NLM	NetWare Loadable Module
NMS	NetWare Management System
NNTP	Network News Transfer Protocol
NOS	Network Operating System
NSA	National Security Agency
NSC	Network Security Center
NSS	Network Security System
NTSL	National Testing Software Laboratories
NUI	NetWare Users International
NWADMIN	NetWare Administrator Graphical Utility
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
POP	Post Office Protocol
RAM	Random Access Memory
RCS	Remote Connect Security
RISC	Reduced Instruction Set Computer
RSA	Rivest, Shamir, and Adleman
SATAN	Security Administrator Tool for Analyzing Networks
SBIR	Small Business Innovation Research
SDNS	Secure Data Network System
SHS	Secure Hash Standard
SILS	Standard for Interoperable LAN and MAN Security
SMDS	Switch Multimegabit Data Service
SMS	Storage Management System
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPAWAR	Space and Naval Warfare Systems Command
SPX	Sequenced Packet Exchange Protocol
STS	Synchronous Transport Signal
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TDY	Temporary Duty Assignment
TTS	Transaction Tracking System
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VEIL	Variable Encryption Intelligent Labeling
VLM	Virtual Loadable Module
V-ONE	Virtual Open Network Environment
WAN	Wide Area Network
WWW	World Wide Web

Appendix B

Points of Contact and Other Resources

This Page Intentionally Left Blank

Appendix B

Points of Contact and Other Resources

Every NetWare administrator requires access to vendor support personnel. Novell provides a number of access points. Novell customer service, sales, training, and other departments can be reached at 1-800-NETWARE. Outside the U.S. and Canada, call 1-801-638-9273.

Novell maintains on-line NetWire forums for users to submit questions to Novell technicians and to share technical ideas with other NetWare administrators. NetWire also has a database of downloadable Novell files and lists of third-party products for NetWare environments. These forums and services are available through the CompuServe Information Service. To subscribe to CompuServe, call 1-800-524-3388, or 614-457-0802, Representative #200, outside the U.S. and Canada.

Through Internet, Novell provides File Transfer Protocol access (`ftp.novell.com`) and World-Wide Web access (`www.novell.com`) to information about their products. Novell provides comprehensive product descriptions on the Web at `http://iamg.novell.com/tree.htm`. These servers are worth browsing from time to time to see what is new.

Discussion lists for NetWare users, administrators, and engineers are maintained on Usenet bulletin boards and are accessible over Internet and other commercial networks using Network News Transfer Protocol (NNTP). Several million people participate in Usenet and dozens of messages are posted daily to the NetWare-relevant discussion lists. Often, a NetWare administrator will have a problem for which they post a question, and they receive several suggestions within hours or days. Novell systems engineers monitor these discussion lists and offer suggestions if other users fail to reply or reply with incorrect solutions. New discussion lists are activated daily and inactive discussion lists are discontinued. At the time of this writing, relevant discussion lists include:

```
bit.listserv.novell
comp.sys.novell
comp.os.netware.announce
comp.os.netware.connectivity
comp.os.netware.misc
comp.os.netware.security
comp.security
comp.security.misc
comp.security.announc
comp.security.pgp
```

Another good source of support for administering NetWare networks is at meetings of fellow NetWare administrators. NetWare User's Groups have been formed in most major cities in the United States and in many cities abroad. For the phone number of the local NetWare User's Group, first contact the NetWare Users International (NUI) at 800-228-4NUI or 801-228-4535 and determine in which regional your city is located. Then call the regional office and ask for the contact in your city. Many local contacts can be made and new ideas exchanged. Guest lecturers are often invited to speak at these meetings. Members of NUI receive the bimonthly publication, *NetWare Connection,* free.

Novell publishes technical bulletins in NetWire regional newsletters. These newsletters are designed to keep the NetWare administrator abreast of changes, upgrades, and training opportunities in their region as well as important topics such as NetWare Security, NetWare for Unix, NetWare in Windows environments, and third-party products which support NetWare. For the phone number of the local regional office in your area, call the nearest regional headquarters: Western United States 1-801-321-7312, Central United States 1-708-956-3535, Eastern United States 1-404-901-6708.

Novell Application Notes (AppNotes) cover topics on network design and optimization strategies, network management tactics, NetWare internals and theory of operations, Novell product implementation guidelines, integration solutions for third-party products, and NetWare programming techniques. AppNotes are published monthly by Novell. AppNotes subscriptions are currently $95 per year (12 issues) inside the United States for hard copy, and $135 outside the United States. Subscribers are also granted access to the electronic version on NetWire for free, plus access charges during downloading. Electronic-only subscriptions are currently $35 annually, plus access charges. Subscriptions can be placed by calling 1-800-377-4136, or 1-303-297-2725 outside the United States. Examples of recent AppNotes include:

- December 1994, Part Number 164-000036-012, topics: NetWare IPX Routing Enhancements, Customizing Your NetWare Link Services Protocol Routing Configuration, Managing Basic MHS, Printing to Network Printers in Windows 3.1, and Configuring UnixWare's Point-to-Point Protocol (PPP).

- September 1994, Part Number 164-000036-009, topics: Using Novell's CDROM.NLM to Run CD-ROM Drives as NetWare Volumes, What's New in NetWare 4.02, Effectively Managing RIP and SAP Traffic with Filtering, UnixWare 1.1 as a NetWare Client, and Troubleshooting Printing in a NetWare for Macintosh Environment.

- July 1994, Part Number 164-000036-007, topics: Configuring NetWare 4 for Mobile User, Key Issues Surrounding Enterprise E-Mail, Testing Performance of NetWare SNA Remote Host Connectivity Products, Customizing Autodiscovery Using NMS, Records Management: Document Storage and Retrieval Challenges in an Enterprise Network, and Application of Networked Multimedia in Business and Education.

Novell Research Reports are specialized reports that cover topical issues in depth. For a listing, or to order these reports, contact Novell Research Order Desk, 1601 Park Avenue West, Denver, CO 80216-5199, or call 1-800-453-12647, extension 5380.

Novell Press publishes references and guides pertaining to NetWare. Novell Press books can be ordered by calling Sybex, Inc., 1-800-227-2346 (international customers: 1-801-429-7177) or writing to Sybex, Inc., 2021 Challenger Drive, Alemeda, CA 94501.

Novell publishes a very useful overview of NetWare and related products in a Buyer's Guide available on the World Wide Web at `http://www.novell.com/SalesMkt/BuyersGuide/Section4.html`.

Many corporations have also developed security "home pages" on the World-Wide Web this year. These sites have pointers to security-related software and references that can be downloaded for free using a Web browser such as Netscape. Examples of security home pages are:

`http://www.tetstra.com.au/pub/docs/security/`

`http://galaxy.einet.net/galaxy/Engineering-and-Technology/Computer-Technology/Security.html`

`http://galaxy.einet.net:80/galaxy/Engineering-and-Technology/Computer-Technology/Security/security-links.html`

`http://saicmgm52.mgm.saic.com/SecurityDocs.html`

`http://mls.saic.com;/docs.html`

`http://home.mcom.com/info/security-doc.html`

`http://home.mcom.com/info/security-overview.html`

`http://www.tis.com`

`http://csrc.ncsl.nist.gov/publications.html`

`http://hightop.nrl.navy.mil/firewall.html`

`http://hoohoo.ncsa.uiuc.edu/docs/PEMPGP.html`

`http://www.greatcircle.com`

`http://www.csi.it/csipages/ebooks.html`

A file of frequently asked questions (FAQ's) about NetWare is updated occasionally and posted at `ftp://midir.ucd.ie/novell/faq.tx`. This file includes instructions on how to subscribe to the LISTSERV mailing list managed by Novell and accessible over Internet and Bitnet. It also provides phone numbers for various departments at Novell.

Another very useful file, available on the World Wide Web at `http://www.sparco.com/mdir.html`, provides a telephone directory of approximately 1,000 manufacturers of computer and communications products. If the company has an 800-number, it is listed. If the company has an bulletin board, Web home page, FTP server, or can be reached by electronic mail, their Internet address is listed.

The Massachusetts Institute of Technology also maintains a list of manufacturer and vendor phone numbers, including bulletin board numbers, with approximately 1,000 entries. The list is available on the World Wide Web at `http://foundation.mit.edu/doc/pc-phonelist.txt`.

Several magazines which are published weekly or monthly devote columns to NetWare bugs, fixes, issues, and third-party products. Subscription information to some of these is as follows:

LAN Times
1900 O'Farrell St., Suite 200, San Mateo, CA 94403
800-525-5003

NetWare Technical Journal
1900 O'Farrell St., Suite 200, San Mateo, CA 94403
800-525-5003

LAN Computing
Cardinal Business Media, Inc., 101 Witmer Rd., Horsham, PA 19044
215-957-4269

MacWeek
P.O. Box 1766, Riverton, NJ 08077-7366
609-461-2100

PC Week
P.O. Box 1770, Riverton, NJ 08077-7370
609-461-2100

Infoworld
P.O. Box 1172, Skokie, IL 60076
800-457-7866

NetWork News
CNE Professional Association, MS #E-31-1, 122 E. 1700 South, Provo, UT 84606
800-926-3776

LAN Magazine
600 Harrison Street, San Francisco, CA 94107
800-234-9573

Network Computing
CMP Publications, 600 Community Drive, Manhasset, NY 11030
516-562-5071

Network World
International Data Group, 6161 Worcester Rd., Framingham, MA 01701
508-875-6400

A free magazine (for those that qualify) which often has articles on NetWare security and publishes lists of vendors and their products is Infosecurity News:

Infosecurity News
498 Concord Street
Framingham, MA 01701
508-879-9792

There are also magazines which are devoted to the latest and greatest on Internet. An excellent magazine on this topic is:

Internet World
Mecklermedia Corp., 20 Ketchum St., Westport, CT 06880
Subscriptions: P.O. Box 713, Mount Morris, IL 61054-9965
800-573-3062, or in the U.K. 0-71-976-0405

Some publishers place their magazines on-line on the World Wide Web. Examples of publisher home pages are:

- `http://techweb.cmp.com:2090/techweb` – includes several magazines from CMP Publications, some of which include articles on NetWare 4. Best of all, this home page has a search tool that allows the user to enter keywords to search for. TechWeb also allows users to subscribe to receive free on-line postings. The subscription form is available at this home page.

- `http://www.zif.com/` – includes approximately a dozen Ziff-Davis magazines for PC and Macintosh users, some of which include articles on NetWare.

- `http://www.cris.com/~milewski/magnet.html/` – provides an index to approximately 100 computer and telecommunications magazines. This is an excellent source!

- `http://www.lanmag.com/cover/cover.html` – LAN Magazine.

- `http://www.mecklerweb.com/` – provides a Web Wide Web guide, information on the Web, and a magazine about the Web.

Another source of information is *video training.* One well known provider of NetWare video training courseware is Wave Technologies International. Wave Technologies is not a Novell Authorized Education Center because Wave does not meet the requirement that they promote only Novell products. Furthermore, the author has not evaluated Wave products and cannot endorse their products. However, many of their trainers are Certified Novell Engineers (CNEs) with current training (NetWare 4.1 at the time of this writing) and Wave has a strong reputation in the field. For information on Wave Technologies courseware, call 800-828-2050 or 314-995-5767 in Missouri. In the U.K. call 0800-393-205 or 081-332-0700.

ON Technology Corporation also has an impressive selection of NetWare training videos. For information, call 800-381-5686, or write to ON Technology Corporation at One Cambridge Center, Cambridge, MA 02142-1604.

Firewall training is available from Great Circle Associates, 1057 W. Dana Street, Mountain View, CA 94041, (800) 270-2562, or `http://www.greatcircle.com/`.

Finally, sources for answering general security questions not relating to NetWare, or for direction to someone who may be able to answer such questions include several commercial associations:

Computer Security Institute – (415) 905-2626

Information Systems Security Association – (708) 699-6441

American Society for Industrial Security – (703) 522-5800.

Appendix C

Recommended Reading

This Page Intentionally Left Blank

Appendix C

Recommended Reading

Every NetWare administrator requires a library of text books and reference manuals to turn to in times of crisis. Of course, the Novell manuals that are delivered with the NetWare Network Operating System and the Novell handbooks that the administrator received while attending training courses are very important. In addition, this appendix suggests a minimum set of commercial references that are particularly useful. The complete bibliography of books and articles that were used to develop this handbook are provided in **Appendix C**.

[CHAPMAN 95] Chapman, D. Brent and E.D. Zwicky, *Building Internet Firewalls,* O'Reilly and Associates, New York, NY, 1995, ISBN: 1-56592-124-0, $29.95.

This book is directed toward the network administrator who is faced with the task of interfacing their organization's LAN with Internet so that electronic mail and other files can be exchanged. This book is scheduled to become available on September 18, 1995 and has not been reviewed for this SBIR effort. However, it is almost two years newer than the Cheswick firewall book below and is expected to be an excellent reference. It can be purchased from Great Circle Associates, 1057 West Dana Street, Mountain View, CA 94041, (800) 270-2562.

[CHES 94] Cheswick, William R. and Steven M. Bellovin, *Firewalls and Internet Security - Repelling the Wily Hacker,* Addison-Wesley, Reading, MA, 1994, ISBN 0-201-63357-4, $24.95. *(Also available via the Internet at ftp://ftp.research.att.com/dist/internet_security/firewall.book.)*

This is a very technical security book that is directed toward the network administrator who is faced with the task of interfacing their organization's LAN with Internet so that electronic mail and other files can be exchanged. Many Navy LANs have this requirement. If your network is being considered for such connectivity, this book is a must.

[FORD 94] Ford, Warwick, *Computer Communications Security – Principles, Standard Protocols and Techniques,* Prentice Hall, Englewood Cliffs, NJ, 1994, ISBN: 0-13-799453-2, $58.00.

Not directed toward NetWare, but toward network security in general. This is for network administrators that have the time and are ready to broaden their horizons by gaining an understanding of the full range of pervasive security services, protocols, mechanisms, and techniques.

Appendix C – Recommended Reading (continued)

[HERBON 94] Herbon, Gamal, *Designing NetWare Directory Services,* Henry Holt and Company, New York, NY, 1994, ISBN: 1-55851-338-8, $29.95.

If you have never planned and set up a NetWare 4 Directory tree, this book is a must. It guides you through planning and installation, including migration from NetWare 3.X.

[HUNTER 93] Hunter, Philip, *Local Area Networks – Making the Right Choices,* Addison-Wesley, Reading, Massachusetts, 1993, ISBN: 0-201-62763-9 $25.25.

An excellent general book on LAN cabling, protocols, servers, and management. Recommended for both the beginner and the advanced network administrator.

[LAWREN 93] Lawrence, Bill, et al., *Using Novell NetWare 4 – Special Edition,* Que Corporation, New York, NY, 1993, ISBN: 1-56529-069-0, $35.00.

A complete NetWare 4 reference manual – probably not a book you want to read from cover to cover, but one that provides short, complete instructions for accomplishing any NetWare 4 administration task.

[NIST 94D] National Institute of Standards and Technology, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls, NIST Special Publication 800-10,* NIST, Gaithersburg, MD, September 1994. This can be picked up for free on the World Wide Web.

An excellent and easy to read introduction to firewall technology. Any Navy organization that is connected to or considering becoming connected to external non-secure networks, such as the Internet, should study this publication. A more comprehensive review of the subject is provided in [CHES 94].

Appendix C – Recommended Reading (continued)

[NOVELL 94R 94S, 94T, 94U, and 94V] Novell, Inc., *NetWare 4 Network Computing Products Series,* Provo, Utah, December 1994.

This five-volume series is the first set of Novell references written specifically for NetWare 4.1. Each volume is approximately 500 pages and is extremely well written. *Concepts* (Novell Part Number 100-002073-001) covers all the basics. *Supervising the Network* (Novell Part Numbers 100-002074-001 and 100-002075-001) and *Print Services* (Novell Part Number 100-002072-001) walk through procedures for using each of the utilities and commands. *Utilities Reference* (Novell Part Number 100-002070-001) lists all utility options, NDS object properties, and other details that an administrator must have access to. *NetWare Client for DOS and MS Windows User Guide* (Novell Part Number 100-002077-001) guides the user in installing and setting up client software and describes User Tools. These are provided to students taking the NetWare 4.X Basic Administrator's Course (Novell course 520), or can be purchased from Novell (800-453-1267 or 801-429-7000).

[NOVELL 94W] Novell, Inc., Gamal B. Herbon, Editor, *Novell Application Notes, 5 (4): Special Edition – Building and Auditing a Trusted Network Environment with NetWare 4,* Novell, Inc., Provo, Utah, April 1994, Novell Part Number 164-000036-004, $15 inside the United States ($20 outside).

This 196 page special report is a Novell Cooperative Research Report written by experts in the field and published by Novell. It covers major audit and security concerns, an overview of network technology, trusted computing and networking specifications for government and commercial organizations, threats and countermeasures, security implementation tips, auditing approaches, and access controls. AppNotes subscriptions and Research Reports are available by calling (800) 377-4136.

[NOVELL 95D] Novell, Inc., David J. Clarke, *Novell's Guide to Network Security,* Provo, Utah, 1995, ISBN 0-7821-1617-5, $44.99.

This was due first quarter 1995 but is not yet available and will not be available in 1995. It will be available from Novell Press Books, 800-227-2346. This is anticipated to be a comprehensive, well-written guide to NetWare 4.1 security.

Appendix C – Recommended Reading (continued)

[SHELDON 94] Sheldon, Tom, et al., *LAN Times Encyclopedia of Networking,* McGraw-Hill, Berkeley, California, 1994, ISBN: 0-07-881965-2, $39.95.

This encyclopedia describes everything from connectors to groupware to compression. Numerous descriptions are provided in terms of NetWare, as well as other network operating systems. Graphics are plentiful. This is another must for every NetWare administrator's library.

[WILCOX 94] Wilcox, Adam, *PC Learning Labs Teaches NetWare,* Ziff-Davis, Emeryville, California, 1994, ISBN: 1-56276-253-2, $22.95.

This simple book is for the NetWare beginner. It covers only NetWare 3.12, but has graphics and is easy to follow. It comes with a diskette that contains a tutorial and sample files to work through while reading the book. It could also be loaned to new users for training.

Appendix D

References

This Page Intentionally Left Blank

Appendix D

References

[ANTHES 94] Anthes, Gary, "Poll finds security less than passable," *Computerworld,* Volume 28, Issue 16, April 18, 1994, pp. 63.

[BAKER 95] Baker, Richard H., *Network Security – How to Plan For It and Achieve It,* McGraw-Hill, New York, NY, 1995.

[BALLOU 93] Ballou, Melinda C., "UnixWare, NetWare Blend Questioned," *Computerworld,* Volume 27, Number 29, July 19, 1993, pp. 14.

[BLACK 93] Black, Uyless, *Data Link Protocols* , Prentice Hall, Englewood Cliffs, NJ, 1993.

[BOCKEN 94] Bockenski, Barbara, *Implementing Production-Quality Client/Server Systems,* John Wiley & Sons, New York, NY, 1994.

[BUSSE 93] Busse, Torsten, "Intel Beefs Up Features of LANDesk Manager – NLMs Offer Node Data, Security," *Infoworld,* Volume 15, Number 25, June 21, 1993, pp. 45.

[CHAP 92] Chapman, D. Brent, "Network (In) Security Through IP Packet Filtering," *USENIX Security Symposium III Proceedings,* USENIX Association, Baltimore, MD, September 14-16, 1992.

[CHAP 95] Chapman, D.B. and E.D. Zwicky, *Building Internet Firewalls,* O'Reilly and Associates, New York, NY, 1995.

[CHES 94] Cheswick, William R. and Steven M. Bellovin, *Firewalls and Internet Security - Repelling the Wily Hacker,* Addison-Wesley, Reading, MA, 1994.

[CHIU 92] Chiu, Dah Ming and Ram Sudama, *Network Monitoring Explained – Design and Applications,* Ellis Horwood Limited, Cirencester, England, 1992.

[CHORA 94] Chorafas, Dimitris N., *Beyond LANS – Client/Server Computing,* McGraw-Hill, New York, NY, 1994.

[COOPER 95] Cooper, F.J. et al., *Implementing Internet Security,* New Riders Publishing, Indianapolis, IN, 1995.

Appendix D – References (continued)

[COOPERS 94] Coopers & Lybrand, *Novell NetWare – Security, Audit, and Control,* presentation notes, Information Systems Audit and Control Association Mid-Atlantic Audit & Control Conference, September 14, 1994.

[COURSEY 93] Coursey, David, "In Need of Novell," *Computerworld,* Volume 27, Number 35, August 30, 1993, pp. 60.

[CRAW 93] Crawford, Tim M., "Install a Secret Back Door to Your Server," *Infoworld,* Volume 15, Number 40, October 4, 1993, pp. 125.

[DALY 92] Daly, James, "Antivirus Utility for NetWare Servers Due," *Computerworld,* Volume 26, Number 47, November 23, 1992, pp. 4.

[DALY 93A] Daly, James, "Applications Offer Central Net Security," *Computerworld,* Volume 27, Number 31A, August 9, 1993, pp. 62.

[DALY 93B] Daly, James, "Open Security: Resolving the Paradox," *Computerworld,* Volume 27, Number 31A, August 11, 1993, pp. 22-26.

[DALY 93C] Daly, James, "Put a Sentry On Your LAN," *Computerworld,* Volume 27, Number 41, October 11, 1993, pp. 44.

[DAVIS 94A] Davis, Peter T., *Complete LAN Security and Control,* McGraw-Hill, New York, NY, 1994.

[DAVIS 94B] Davis, Peter T., *Manager's Guide to Internet Security,* Computer Security Institute, San Francisco, CA, 1994.

[DAY 92] Day, Michael, *Enterprise Series: Downsizing to NetWare,* New Riders Publishers, Carmel, Indiana, 1992.

[DECISIS 94] Decisis, Inc., *1995 Guide to Switched Internetworking Technologies,* Decisis, Inc., Herndon, VA, 1994.

[DEWIRE 94] Dewire, Dawna T., *Application Development for Distributed Environments,* McGraw-Hill, New York, NY, 1994.

[DOSTER 92A] Dostert, Michele, "Microsoft, Novell Square Off," *Computerworld,* Volume 26, Number 47, November 23, 1992, pp. 6.

[DOSTER 92B] Dostert, Michele, "Novell Issues Network Security Patch – Device Will Guard Against LAN Break-ins But Not Careless Users," *Computerworld,* Volume 26, Number 47, November 23, 1992, pp. 4.

Appendix D – References (continued)

[ELLISON 92] Ellison, Craig, "Intel Joins the Network Virus Hunt with LANProtect," *PC Magazine,* Volume 11, Number 1, June 16, 1992, pp. 50.

[FATAH 94] Fatah, Burhan, *Electronic Mail Systems – A Network Manager's Guide,* McGraw-Hill, New York, NY, 1994.

[FIREFOX 95] Firefox, Inc., *Internet Security: Solutions for the NetWare Environment,* Firefox, Inc., San Jose, CA, March 1995.

[FORD 94] Ford, Warwick, *Computer Communications Security – Principles, Standard Protocols and Techniques,* Prentice Hall, Englewood Cliffs, NJ, 1994.

[FRYER 94] Fryer, Bronwyn, "Virus Protection: At Your Server," *Computerworld,* Volume 28, Number 18, May 2, 1994, pp. 121.

[GHIGG 93] Ghiggino, Pierpaolo and Charles A. Eldering, Editors, *Local and Metropolitan Area Networks,* SPIE – The International Society for Optical Engineering, Bellingham, WA, 1993.

[HALSALL 92] Halsall, Fred, *Data Communications, Computer Networks and Open Systems,* Third Edition, Addison-Wesley Publishing Company, Reading, Massachusetts, 1992.

[HAMPTON 93] Hampton, William R., "Improving LAN Security and Auditing Using Novell NetWare Version 4.0," *Computer Security Journal,* Volume 9, Number 2, Fall 1993, pp. 37-47.

[HARBAUG 93] Harbaugh, Logan G., *Novell's Problem-Solving Guide to NetWare Systems,* Novell Press, San Jose, CA, 1993.

[HELD 94] Held, Gilbert, *Token-Ring Networks: Characteristics, Operations, Construction, and Management,* John Wiley & Sons, New York, NY, 1994.

[HERBON 94] Herbon, Gamal, *Designing NetWare Directory Services,* Henry Holt and Company, New York, NY, 1994.

[HOFFMAN 93] Hoffman, Thomas, "Novell Leads Client/Server Security Effort," *Computerworld,* Volume 27, Number 29, July 19, 1993, pp. 14.

[HORWITT 93] Horwitt, Elizabeth, "Interop '93 Unveilings – Products Demonstrate Vendors' Commitment to SNMP Systems, Interoperability Across Systems," *Computerworld,* Volume 27, Number 35, August 30, 1993, pp. 59.

Appendix D – References (continued)

[HORWITT 94] Horwitt, Elizabeth, "LAN/Mainframe Security Addressed," *Computerworld,* Volume 28, Number 12, March 21, 1994, pp. 69.

[HUNTER 93] Hunter, Philip, *Local Area Networks – Making the Right Choices,* Addison-Wesley, Reading, Massachusetts, 1993.

[IEEE 94] Institute of Electrical and Electronics Engineers, *IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS) Clause 3 — Key Management Protocol,* Unapproved Draft IEEE 802.10c/D5, June 8, 1994.

[INFOSEC 94] "Encryption: Scramble Data to Protect It," *Infosecurity News,* November/December, 1994, pp. 82-91.

[ISO 89] International Standards Organization, *Information Processing Systems — Open Systems Interconnection Basic Reference Model — Part 2: Security Architecture*, ISO 7498-2, February 1989.

[JOHNSON 94] Johnson, Johna T., "The Internet: Corporations Worldwide Make the Connection," *Data Communications,* Volume 23, Number 6, April, 1994, pp. 66-78.

[JOST 92] Jost, Marty, *NetWare – The Macintosh Connection,* Windcrest-McGraw-Hill, Blue Ridge Summit, PA, 1992.

[KAPLAN 95] Kaplan, Jon, "Unscrambling the Secret of Encryption," *Security Management,* Volume 39, Number 2, February, 1995, pp. 67-70.

[KAVAN 95] Kavanagh, Paul, *Downsizing for Client/Server Applications,* Academic Press Professional, Cambridge, MA, 1995.

[KING 94] King, Adrian, "Examining the Peer-to-Peer Connectivity and Multiple Network Support of Chicago," *Microsoft Systems Journal,* Volume 9, Number 11, November, 1994, pp. 15-30.

[LAN 95] LAN – The Network Solutions Magazine, *1995 Buyers Guide Issue,* Miller Freeman Publication, Boulder, CO, October, 1995.

[LAUBACH 93] Laubach, Edwin G., et al., *Networking with Banyan VINES, Second Edition,* McGraw-Hill, New York, NY, 1993.

[LAWREN 93] Lawrence, Bill, et al., *Using Novell NetWare 4 – Special Edition,* Que Corporation, New York, NY, 1993.

Appendix D – References (continued)

[LAWREN 94] Lawrence, Bill, et al., *Using NetWare 3.12 – Special Edition,* Que Corporation, New York, NY, 1994.

[LIEBING 93] Liebing, Edward, *NetWare User's Guide, Versions 3.11 and 3.12,* Henry Holt and Company, New York, NY, 1993.

[MADRON 92] Madron, Thomas W., *Network Security in the '90s – Issues and Solutions for Managers,* John Wiley & Sons, New York, NY, 1992.

[MARSH 94] Marshall, Brian, *Using Windows NT: The Essentials for Professionals,* Prentice-Hall, Englewood Cliffs, NJ, 1994.

[MARTIN 94] Martin, James, *Local Area Networks – Architectures and Implementations, Second Edition,* Prentice Hall, Englewood Cliffs, NJ, 1994.

[MCCAR 93] McCarthy, Vance, "NetWare Add-in Closes Password Detection Loophole On Small LANs," *Infoworld,* Volume 15, Number 36, September 6, 1993, pp. 8.

[MEREN 94] Merenbloom, Paul, "LAN Talk – Some Tips For Smoothly Upgrading Your Server to NetWare 4," *Infoworld,* Volume 16, Number 21, May 23, 1994, pp. 94.

[MIAST 93] Miastkowski, Stan and Anne Fischer Lent, *The Windows for Workgroups Bible,* Addison-Wesley, Reading, MA, 1993.

[MICRO 92] Microsoft Corporation, *WG0667: Peer-to-Peer vs. Client-Server Networks,* Application Notes – Windows for Workgroups Version 3.1 Resource Kit, 1992.

[MULLER 93] Muller, Nathan J., *Intelligent Hubs,* Artech House, Inc., Boston, MA, 1993.

[NIEDER 94] Niedermiller-Chaffins, Debra, and Dorothy Cady, *NetWare Training Guide: Managing NetWare Systems, Second Edition,* New Rider Publishing, Indianapolis, Indiana, 1994.

[NIST 91] National Institute of Standards and Technology, "Advanced Authentication Technology," *CSL Bulletin,* NIST, Gaithersburg, MD, November 1991.

[NIST 92] Polk, W.T. and L.E. Bassham, *A Guide to the Selection of Anti-Virus Tools and Techniques,* NIST, Gaithersburg, MD, December 2, 1992.

Appendix D – References (continued)

[NIST 93A] National Institute of Standards and Technology, "Connecting to the Internet: Security Considerations," *CSL Bulletin,* NIST, Gaithersburg, MD, July 1993.

[NIST 93B] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Message Security Protocol (MSP),* SDN.701, Revision 2.1, NIST, Gaithersburg, MD, November 23, 1993.

[NIST 94A] National Institute of Standards and Technology, "Reducing the Risk of Internet Connection and Use," *CSL Bulletin,* NIST, Gaithersburg, MD, May 1994.

[NIST 94B] National Institute of Standards and Technology, *Advanced Authentication Technology Alternatives, Federal Information Processing Standard 190 (FIPS 190),* NIST, Gaithersburg, MD, September 1994.

[NIST 94C] National Institute of Standards and Technology, *Security in Open Systems, NIST Special Publication 800-7,* NIST, Gaithersburg, MD, September 1994.

[NIST 94D] National Institute of Standards and Technology, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls, NIST Special Publication 800-10,* NIST, Gaithersburg, MD, September 1994.

[NIST 94E] National Institute of Standards and Technology, *Escrowed Encryption Standard, Federal Information Processing Standard 185 (FIPS 185),* NIST, Gaithersburg, MD, February 1994.

[NOVELL 90] Novell, Inc., *NetWare System Interface Technical Overview,* Addison-Wesley, Reading, Massachusetts, 1990.

[NOVELL 91] Novell, Inc., *NetWare Security: Configuring and Auditing a Trusted Environment,* Novell, Inc., Provo, Utah, 1991.

[NOVELL 93A] Novell, Inc., *NetWare Global Security Architecture – White Paper,* Novell, Inc., Provo, Utah, July 1993.

[NOVELL 93B] Novell, Inc., Laura Chappell, *Novell's Guide to Multiprotocol Internetworking* Novell, Inc., Provo, Utah, November 1993.

[NOVELL 93C] Novell, Inc., Logan Harbaugh, *Novell's Problem-Solving Guide for NetWare Systems,* Novell, Inc., Provo, Utah, September 1993.

Appendix D – References (continued)

[NOVELL 93D] Novell, Inc., Cheryl Currid, *Novell's Guide to NetWare 4 Networks,* Novell, Inc., Provo, Utah, April 1993.

[NOVELL 93E] Novell, Inc., *Novell's Application Notes for NetWare 4,* Novell, Inc., Provo, Utah, September 1993.

[NOVELL 94A] Novell, Inc., Alan Mark, *Novell's Corporate-Wide Upgrade to NetWare 4,* Novell, Inc., Provo, Utah, January 1994.

[NOVELL 94B] Novell, Inc., Larry E. Morris, *Upgrading to NetWare 4: The Chase Manhattan Bank's Corporate Controllers and Financial Management Information Groups – A Novell Research Case Study,* Novell, Inc., Provo, Utah, January 1994.

[NOVELL 94C] Novell, Inc., Marcus Williamson, *Time in the NetWare Environment,* Novell, Inc., Provo, Utah, January 1994.

[NOVELL 94D] Novell, Inc., Myron Mosbarger, *Computer-Telephone Integration with Novell's Telephony Services,* Novell, Inc., Provo, Utah, January 1994.

[NOVELL 94E] Novell, Inc., Dan Stuart, *An Overview of Multimedia Technologies,* Novell, Inc., Provo, Utah, January 1994.

[NOVELL 94F] Novell, Inc., *NetWare Directory Services Rules of Thumb,* Novell, Inc., Provo, Utah, created July 8, 1993, printed February 9, 1994.

[NOVELL 94G] Novell, Inc., *NetWare 4 Consultant's Conference – Migration Technical Track,* briefing slides, Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94H] Novell, Inc., J. Orland Seaver, *Implementing Naming Standards for NetWare Directory Services,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94J] Novell, Inc., J. Orland Seaver, *TimeSync – What is Left,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94K] Novell, Inc., Jeff Hughes and Blair Thomas, *Understanding and Using Object Rights: Detailed Script,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94L] Novell, Inc., Carl Seaver, *Quick Path to NetWare 4 – Migration, Compatibility and Operations,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94M] Novell, Inc., *NetWare 4 Implementation Plan – High Level Project Plan and Approach,* Novell, Inc., Provo, Utah, February 1994.

Appendix D – References (continued)

[NOVELL 94N] Novell, Inc., *NetWare 4 Transitional Briefing – Program Guide,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94P] Novell, Inc., *NetWare 4 Quick Start Implementation Guide, Revision 1.0,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94Q] Novell, Inc., *NetWare Features Comparison Guide,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94R] Novell, Inc., *NetWare 4 Network Computing Products: Concepts,* Provo, Utah, December 1994.

[NOVELL 94S] Novell, Inc., *NetWare 4 Network Computing Products: Supervising the Network, Volumes 1 and 2,* Provo, Utah, December 1994.

[NOVELL 94T] Novell, Inc., *NetWare 4 Network Computing Products: Print Services,* Provo, Utah, December 1994.

[NOVELL 94U] Novell, Inc., *NetWare 4 Network Computing Products: Utilities Reference,* Provo, Utah, December 1994.

[NOVELL 94V] Novell, Inc., *NetWare 4 Network Computing Products: NetWare Client for DOS and MS Windows User Guide,* Provo, Utah, December 1994.

[NOVELL 94W] Novell, Inc., Gamal B. Herbon, Editor, *Novell Application Notes, 5 (4): Special Edition – Building and Auditing a Trusted Network Environment with NetWare 4,* Novell, Inc., Provo, Utah, April 1994.

[NOVELL 94X] Novell, Inc., Laura Chappell, *Novell's Guide to NetWare LAN Analysis, 2nd Edition,* Novell, Inc., Provo, Utah, 1994.

[NOVELL 94Y] Novell, Inc., Michael Day, *Novell's Guide to NetWare 4 NLM Programming,* Novell, Inc., Provo, Utah, 1994.

[NOVELL 94Z] Novell, Inc., Peter Dyson, *Novell's Dictionary of Networking,* Novell, Inc., Provo, Utah, 1994.

[NOVELL 94AA] Novell, Inc., Werner Feibel, *Novell's Complete Encyclopedia of Networking,* Novell, Inc., Provo, Utah, November 1994.

[NOVELL 95A] Novell, Inc., Jeff Hughes, *Novell's Quickpath to NetWare 4.1,* Provo, Utah, 1995.

[NOVELL 95B] Novell, Inc., James E. Gaskin, *Novell's Complete Guide to NetWare 4.1,* Novell, Inc., Provo, Utah, June 1995.

Appendix D – References (continued)

[NOVELL 95C] Novell, Inc., and Intel Network Technology, *White Paper – ManageWise: The Smart Way to Manage Your Network,* Novell, Inc., Provo, Utah, January 1995.

[NOVELL 95D] Novell, Inc., David J. Clarke, *Novell's Guide to Network Security,* Provo, Utah, 1995. (Note: was due first quarter 1995 but not yet available at this writing; will be available from Novell Press Books, 1-800-227-2346; ISBN 0-7821-1617-5, $44.99)

[NSA 94] National Security Agency, *MOSAIC Program Overview, Version 2,* January 28, 1994.

[NTSL 93] National Testing Software Laboratories, *Virus Prevention NLMs,* 1993; (published in Software Digest, Volume 11, Number 5, May 1994 and Byte, August 1994).

[POLILLI 94A] Polilli, Steve, "Client/Server Gets Antiviral Software," *Infoworld,* Volume 16, Number 21, May 23, 1994, pp. 58.

[POLILLI 94B] Polilli, Steve, and Shawn Willett, "Intel Integrates Management – NetWare Distributed Management System Lacks APPS and Frustrates Interested Users," *Infoworld,* Volume 16, Number 8, February 21, 1994, pp. 10.

[QUARTER 94] Quarterman, J.S. and S. Carl-Mitchell., *The Internet Connection: System Connectivity and Configuration,* Addison-Wesley Publishing Company, Reading, MA, 1994.

[RADDING 93] Radding, Alan, "Dial-up Routers – Low-cost Dial-up Routers Provide Full-fledged Internetworking to Remote Corporate Sites," *Infoworld,* Volume 15, Number 46, November 15, 1993, pp. 67-68.

[RANUS 92] Ranus, Marcus J., *A Network Firewall,* Digital Equipment Corporation, Washington Open Systems Resource Center, Greenbelt, MD, available on World Wide Web, June 12, 1992.

[RANUS 93] Ranus, Marcus J., "Thinking About Firewalls," *Proceedings of Second International Conference on Systems and Network Security and Management (SANS-II),* available on World Wide Web, April 1993.

[RANUS 94] Ranus, Marcus J. and Frederick M. Avolio, *A Toolkit and Methods for Internet Firewalls,* Trusted Information Systems, available on World Wide Web, 1994.

Appendix D – References (continued)

[RASH 90] Rash, Wayne and Peter R. Stephenson, *The Novell Connection,* Simon and Schuster, New York, NY, 1990.

[ROTHKE 94] Rothke, Ben, "Peer to Peer – SmartPass NLM Makes Converts Out of End-users With Insecure Passwords," *Infoworld,* Volume 16, Number 20, May 16, 1994, pp. 49.

[RUNYAN 95] Runyan, Pete, "Special Report: NetWare Security – All Quiet on the NetWare Front," *LAN: The Network Solutions Magazine,* Volume 10, Number 11, October 1995, pp. 142-147.

[SASSER 92] Sasser, Susan, et al., *Troubleshooting Your LAN,* Henry Holt and Company, New York, NY, 1992.

[SAUNDER 94] Saunders, Stephen, "What Is Your LAN Vendor Doing About Security? – The Leading Suppliers of LAN Operating Systems Are Taking Different Approaches to Keep Networks Safe From Harm," *Data Communications,* Volume 23, Number 6, April, 1994, pp. 107-113.

[SAWICKI 92] Sawicki, Ed, *LAN Desktop Guide to Security – NetWare Edition,* SAMS, Prentice-Hall, Carmel, Indiana, 1992.

[SCHNEIER 94] Schneier, Bruce, *Applied Cryptography – Protocols, Algorithms, and Source Code in C,* John Wiley & Sons, New York, New York, 1994.

[SHELDON 94] Sheldon, Tom, et al., *LAN Times Encyclopedia of Networking,* McGraw-Hill, Berkeley, California, 1994.

[SIYAN 95] Siyan, S. and C. Hare, *Internet Firewalls and Network Security,* New Riders Publishing, Indianapolis, Indiana, 1995.

[STALLING 94] Stallings, William, "Kerberos Keeps the Enterprise Secure," *Data Communications,* Volume 23, Number 12, October 1994, pp. 103-111.

[STANG 93] Stang, David and Sylvia Moon, *Network Security Secrets,* International Data Group Books Worldwide, San Mateo, California, 1993.

[STEPHEN 94] Stephenson, Peter, "Going Underground for Security," *LAN Times,* Volume 11, Number 10, May 23, 1994, pp. 56.

[STEVENS 94] Stevens, W. Richard, *TCP/IP Illustrated, Volume 1,* Addison-Wesley, Reading, MA, 1994.

[STROM 94] Strom, David, "If you think your network security is bad, it's probably worse," *InfoWorld,* Volume 16, Issue 44, October 31, 1994.

Appendix D – References (continued)

[TROCINO 94] Trocino, Richard B., *The Illustrated Guide to NetWare Btrieve 6.x,* Golden West Products International, Sherman Oaks, CA, 1994.

[VANKIRK 93] Van Kirk, Doug, "Data Encryption Facilitates Confidentiality," *Infoworld,* Volume 15, Number 12, March 22, 1993, pp. 62.

[WILCOX 94] Wilcox, Adam, *PC Learning Labs Teaches NetWare,* Ziff-Davis, Emeryville, California, 1994.

[WILLETT 93] Willett, Shawn, "Antivirus NetShield Adds Tuning, Spots Suspicious Activity," *Infoworld,* Volume 15, Number 41, October 11, 1993, pp. 46.

[WILLETT 94] Willett, Shawn, "Novell Adds TCP/IP Support, Security to VLM," *Infoworld,* Volume 15, Number 52-1, December 27, 1993 / January 3, 1994, pp. 10.

[WILSON 93A] Wilson, Jayne, "Banyan to Enhance Its Enterprise Network Services for NetWare," *Infoworld,* Volume 15, Number 25, June 21, 1993, pp. 45.

[WILSON 93B] Wilson, Jayne, and Shawn Willett, "HP, Novell Unite Management; Effort Will Boost Network Security, Software Delivery," *Infoworld,* Volume 15, Number 44, November 1, 1993, pp. 3.

[WILSON 93C] Wilson, Jayne, and Shawn Willett, "IBM to Add DCE Directory Services to NetWare 3.X; NLM is Featured in Distribution Plan," *Infoworld,* Volume 15, Number 47, November 22, 1993, pp. 1, 103.

This Page Intentionally Left Blank